Datenschutz und Technikgestaltung

Geschichte und Theorie des Datenschutzes aus informatischer Sicht
und Folgerungen für die Technikgestaltung

D I S S E R T A T I O N

zur Erlangung des akademischen Grades
Dr. rer. nat.

im Fach Informatik

eingereicht an der
Mathematisch-Naturwissenschaftlichen Fakultät
der Humboldt-Universität zu Berlin

von
Diplom-Informatiker Jörg Pohle

Präsidentin der Humboldt-Universität zu Berlin
Prof. Dr.-Ing. Dr. Sabine Kunst

Dekan der Mathematisch-Naturwissenschaftlichen Fakultät
Prof. Dr. Elmar Kulke

Gutachter:
1. Prof. Dr. rer. nat. Wolfgang Coy, HU Berlin
2. Prof. Dr. rer. nat. Ernst-Günter Giessmann, HU Berlin
3. Prof. Dr. jur. Kai von Lewinski, Universität Passau

eingereicht am: 10. August 2016
Tag der mündlichen Prüfung: 08. November 2017

Abstract

The aim of this thesis is to uncover the historical construction of the data protection problem, of data protection as its (abstract) solution, as well as the architecture of its legal implementation, in order to critically assess this construction and to draw conclusions for the design of ICT systems. The thesis reveals which concepts of humankind and society, organizations, information technology and information processing, which informatics, information science, sociological and jurisprudential concepts, schools of thought and theories, and which scientific and pre-scientific assumptions and premises underlie the analysis of the data protection problem, and how they have influenced the specific solution of this problem. Based on a critical assessment of this construction the thesis concludes that data protection must be re-derived as a solution for the information power problem, which is generated by the industrialization of social information processing, and presents an abstract, state-of-the-art data protection attacker model, an analytical framework for a data protection impact assessment as well as a procedural operationalization approach illustrating the sequence as well as the substantive issues to be examined and addressed in this process. The thesis then draws conclusions for the design of data protection friendly—and not necessarily just legally compliant—ICT systems.

Using the approach of a historical systems analysis, the thesis presents a comprehensive examination of the debates concerning the description, classification, and explanation of the problems relating to privacy, data protection, and surveillance, the solutions proposed, their implementation in law and in practice, as well as the debates around the appropriate design of ICT systems. Even though the participants of this debate are using the same set of terms, the thesis shows that the phenomena, practices, and problems addressed by different theories and schools of thought are fundamentally different and, at times, incompatible. These differences relate to the properties and interests ascribed to the actors involved, the purposes and goals they are deemed to pursue, their relationship with each other, but also by which normative standards the information practices of individuals, groups and organizations are to be measured. Consequently, these theories and schools of thought come to wildly different conclusions about what needs to be understood as a problem, how it is to be described and explained, and how it needs to be solved. The thesis also makes clear that there is a lack of consented or even consistently disclosed attacker and threat models in the data protection related systems engineering debate. Besides, many concepts referred to in the debate are either plain wrong, outdated or inadmissibly simplified. This includes the fixation on personally identifiable information, both in terms of the limitation of the scope of application as well as as a reference point for lawmaking and ICT design, the patently false but widespread assertion that sensitivity is a property of information, the naïve public–private dichotomy, the concept of informed consent, especially in its current implementation on the books and on the ground, and the so-called »privacy paradox«.

Zusammenfassung

Ziel der vorliegenden Arbeit ist es, die historische Konstruktion des Datenschutzproblems, des Datenschutzes als seiner (abstrakten) Lösung sowie die Architektur seiner rechtlichen Implementation aufzudecken und einer kritischen Revision aus informatischer Sicht zu unterziehen, um daraus Folgerungen für die Technikgestaltung zu ziehen. Die Arbeit legt offen, welches Verständnis vom Menschen und von der Gesellschaft, von Organisationen, von der Informationstechnik und von der Informationsverarbeitung, welche informatischen, informationswissenschaftlichen, soziologischen und rechtswissenschaftlichen Konzepte, Denkschulen und Theoriegebäude und welche wissenschaftlichen und vorwissenschaftlichen Annahmen und Prämissen der Analyse des Datenschutzproblems zugrunde liegen und wie sie darüber hinaus die spezifische Lösung des Datenschutzproblems – den Datenschutz – gespeist haben. Auf der Basis einer informatisch fundierten Kritik zieht die Arbeit den Schluss, dass der Datenschutz als Lösung des durch die Industrialisierung der gesellschaftlichen Informationsverarbeitung erzeugten Datenmachtproblems neu abgeleitet werden muss, und legt dafür ein dem Stand der wissenschaftlichen Debatte entsprechendes, abstraktes – und damit jeweils noch anwendungsbereichsspezifisch zu konkretisierendes – Datenschutz-Angreifermodell, ein analytisches Raster für eine darauf aufbauende Bedrohungsanalyse sowie einen prozeduralen Operationalisierungsansatz, der die Vorgehensweise und die jeweils zu analysierenden oder zu prüfenden inhaltlichen Fragen deutlich werden lässt, vor. Abschließend zieht die Arbeit Folgerungen für die Gestaltung datenschutzfreundlicher – und dabei nicht notwendig nur datenschutzrechtskonformer – informationstechnischer Systeme.

Die Arbeit legt dazu eine umfassende Untersuchung der politischen und wissenschaftlichen Auseinandersetzungen zur Beschreibung, Einordnung und Begründung der Probleme, die mit den Begriffen *privacy*, Datenschutz und *surveillance* markiert werden, der jeweils vorgeschlagenen Lösungen oder Lösungsansätze, der Umsetzungen dieser Lösungen im Recht und ihrer Anwendung in der Praxis sowie der parallel geführten Debatten um eine zur Lösung dieser Probleme geeignete und angemessene Technikgestaltung in Form einer historischen Systemanalyse vor. Sie legt dabei offen, dass die Unterschiede so groß und teilweise so grundlegend sind, dass die adressierten Phänomene, Praxen und Probleme als voneinander grundsätzlich verschieden verstanden werden müssen, auch wenn sie mit den gleichen Begriffen bezeichnet werden. Diese Unterschiede beziehen sich sowohl auf den betrachteten Gegenstandsbereich, die zugrunde gelegten Akteurskonstellationen, die Eigenschaften und Interessen der Akteurinnen und die von ihnen verfolgten Zwecke, aber auch auf die Zielvorstellungen, an denen sich das Informationsgebaren von Individuen, Gruppen und Organisationen messen lassen muss. Die einzelnen Theorien oder Theorieschulen kommen deshalb zu ganz unterschiedlichen Schlussfolgerungen darüber, was als Problem verstanden werden muss, wie es zu beschreiben und zu erklären ist und wie es gelöst werden muss. Die Arbeit macht zugleich deutlich, dass es im Bereich der Diskussion um die Technikgestaltung an konsentierten oder auch nur durchgängig offengelegten Angreifer- und Bedrohungsmodellen mangelt. Dabei sind viele Konzepte, mit denen in der Debatte operiert wird, aus informatischer Sicht schlicht falsch, überholt oder unzulässig verkürzt. Dazu gehören etwa die Fixierung auf personenbezogene Informationen sowohl hinsichtlich der Beschränkung des Gegenstandsbereichs als auch als Anknüpfungspunkt für Rechtsetzung und Technikgestaltung, die offenkundig falsche und doch weitverbreitete Behauptung, Sensitivität sei eine Eigenschaft von Informationen, die naive Trennung von „öffentlich“ und „privat“, das Konstrukt der informierten Einwilligung, vor allem in seiner derzeitigen Umsetzung, oder das sogenannte „Privacy Paradox“.

„Es geht nicht um Privatsphäre, sondern es geht darum,
eine Technik sozial beherrschbar zu machen. Und das ist alles!“
in memoriam Wilhelm Steinmüller (1934–2013)

Datenschutz ist die Lösung für das „technik-vermittelte gesellschaftliche“ Problem der
„Feststellung und Durchsetzung der Bedingungen, unter denen das Informationsgebaren
einer Gesellschaft für die Glieder der Gesellschaft akzeptabel sein kann.“
in memoriam Adalbert Podlech (1929–2017)

Inhaltsverzeichnis

0 Vorwort und Danksagung

Die vorliegende Arbeit entstand während meiner Zeit in der Arbeitsgruppe „Informatik in Bildung und Gesellschaft“ bei Wolfgang Coy am Institut für Informatik der Humboldt-Universität zu Berlin (HU) und im Forschungsbereich „Globaler Konstitutionalismus und das Internet“ bei Ingolf Pernice am Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG) in Berlin. Sie wurde im August 2016 als Dissertation an der Mathematisch-Naturwissenschaftlichen Fakultät der Humboldt-Universität zu Berlin eingereicht, im September 2017 angenommen und im November 2017 verteidigt.

An erster Stelle möchte ich Wolfgang Coy danken, nicht nur für die Möglichkeit, diese Arbeit bei ihm und in der Arbeitsgruppe zu schreiben, sondern vor allem für die große akademische Freiheit, die er gewährt hat. Nicht zuletzt will ich ihm für sein nie versiegendes Vertrauen in meine am Ende erfolgreich verlaufende Grabung durch Jahrzehnte mäandernder Debatten, verschütteter Diskursströmungen und ex-post erzeugter Narrative danken und seine immer wieder erhellenden Hinweise auf die Kontexte vergangener Auseinandersetzungen sowie die Hintergründe beteiligter Personen.

Ernst-Günter Giessmann möchte ich für sein Zweitgutachten danken und darüber hinaus vor allem für die prägende Kraft seines immerwährenden Insistierens auf ein kritisches Hinterfragen von zugrunde gelegten Annahmen bei der Analyse von IT-Sicherheit in Prozessen und Systemen.

Und ich möchte meinem dritten Gutachter, Kai von Lewinski, danken, der sich als Jurist und Rechts-, vor allem Datenschutzrechtshistoriker bereiterklärt hat, eine zwar interdisziplinäre, aber doch vor allem in der Informatik verortete Dissertation zu begutachten. Seine Arbeiten und seine Bereitschaft, mit mir über Datenschutzgeschichte, -theorie und -recht zu diskutieren, haben wichtige Bausteine für meinen Erkenntnisprozess geliefert.

Desweiteren gilt mein Dank Ingolf Pernice, der in seinem Forschungsbereich am HIIG eine sehr herzliche und wunderbar erkenntnisfördernde Umgebung geschaffen hat, für die Möglichkeit daran teilhaben zu können, für seine hilfreichen Fragen zu den Zusammenhängen und den disziplinübergreifenden Anschlüssen sowie für die große Unterstützung auf dem Weg.

Ganz besonders möchte ich Michael Plöse, der in langen Jahren als Freund und Schreibtischnachbar dafür gesorgt hat, dass ich bei Verstand bleibe, für die vielen produktiven Diskussionen zu einzelnen Teilen und dem Großen und Ganzen danken, und ohne den die Arbeit nicht erfolgreich gewesen wäre.

Martin Rost danke ich für seine nimmermüde Bereitschaft zu Diskussionen über Theorie und Theoriegeschichte des Datenschutzes, seine stets ebenso fundierte wie hilfreiche Kritik an meinen Theorieversuchen und seine kostbaren Hinweise für meinen Einstieg in die soziologische Systemtheorie.

Und nicht zuletzt möchte ich meinen Kolleginnen und Kollegen danken, der Arbeitsgrupe „Informatik in Bildung und Gesellschaft“, vor allem Andrea Knaut, Agata Królikowski, Christian Ricardo Kühne, Rainer Rehak und Stefan Ullrich, und am HIIG, vor allem Marie-Christine Dähn, Maximilian von Grafenstein, Julian Hölzel, Ulrike Höppner, Paula Kift, Hannfried Leisterer, Sebastian Leuschner, Emma Peters, Osvaldo Saldías und Rüdiger Schwarz.

Ein besonderer Dank geht an meine Familie für die große Unterstützung und das Vertrauen.

1 Einleitung

Diese Arbeit verfolgt das Ziel, dem Major Consensus Narrative zum Datenschutz zu widersprechen.

Obwohl dies noch viel mehr für *privacy*, Privatheit oder Privatsphäre gilt, ist auch Datenschutz ein „essentially contested concept“.[1] Es gibt weder in der wissenschaftlichen noch in der politischen Debatte eine Einigung zu den unzähligen Aspekten, die grundlegend für das Verständnis der Problemlage und die Entwicklung von Lösungsansätzen sind. Schon auf der Ebene der Bestimmung des Phänomenbereichs gibt es massive Diskrepanzen zwischen den Beschreibungen, Einordnungen und Erklärungen, die von verschiedener Seite geliefert werden. Während am einen Ende des Spektrums zwischenmenschliche Beziehungen zum Ausgangspunkt der Analyse gemacht werden, richtet sich der Blick am anderen Ende des Spektrums auf die strukturellen Bedingungen der modernen, funktional differenzierten Gesellschaft. Nicht überraschend ist es daher, dass es auch keine Einigung über das Schutzgut gibt: Von individuellen Bedürfnissen oder Interessen wie Privatheit, Vertraulichkeit, Eigentum, Entscheidungsfreiheit oder Persönlichkeitsentfaltung über soziale Konstruktionen wie Menschenwürde, Fairness oder Kommunikationsschutz bis hin zu gesellschaftlichen oder strukturellen Eigenschaften wie Freiheitsräumen, der Informationsordnung oder der Aufrechterhaltung der funktionalen Differenzierung der Gesellschaft wird alles vertreten. Gleiches gilt für die möglichen Gründe, Auslöser oder Verstärker der Gefährdung der betreffenden Schutzgüter. Ob technische Artefakte wie Daten, Informationen oder gar der Computer selbst, Praktiken wie Überwachung oder Veröffentlichung, Verdatung oder Missbrauch, Informationsverarbeitung oder -nutzung, Akteurskonstellationen oder deren Eigenschaften wie Machtimbalancen oder Phänomene auf der gesellschaftlichen Ebene wie die Digitalisierung aller Lebensbereiche, die globale Vernetzung oder die Industrialisierung der gesellschaftlichen Informationsverarbeitung – alles ist schon einmal als Gefahr oder Gefährder, Risiko oder Risikoquelle identifiziert worden. Allein beim rechtlichen Ansatzpunkt scheint sich eine große Mehrheit für das gleiche Schutzobjekt entschieden zu haben: „personenbezogene Daten“; auch wenn es sowohl Streit um deren Geeignetheit gibt als auch keineswegs alle Beteiligten das gleiche darunter verstehen wollen und daher unterschiedliche Daten- und Informationsbegriffe miteinander konkurrieren. Die Regelungsarchitektur hingegen ist, wie sollte es anders sein, wieder fundamental umstritten: von schutzgutorientierten Ansätzen über vertragsorientierte, informationsverarbeitungsorientierte oder informationsflussorientierte Ansätze bis hin zu Ansatzmixen oder besser -sammelsurien. Die Grundregel kann dabei sowohl „Verbot mit Erlaubnisvorbehalt“, das entspricht dem Prinzip „default deny“ bei Firewalls, oder „Erlaubnis mit Verbotsvorbehalt“ („default accept“) lauten. Umgesetzt werden sollen diese Ansätze, so ihre Vertreterinnen und Vertreter, dann wahlweise als formelles oder materielles Recht, durch den Markt oder durch Technik, durch die Verarbeiterinnen und Verarbeiter oder durch die Betroffenen selbst. Und nicht zuletzt sind unzählige unterschiedliche Bezeichner in Gebrauch: Datenschutz – und seine Übersetzungen in verschiedene Sprachen: *data protection*, *protection des*

[1] Siehe zum Begriff grundlegend Gallie (1956). Den Nachweis, dass diese Aussage nicht nur eine Behauptung ist, haben nach der Einreichung dieser Arbeit Mulligan et al. (2016) zumindest für *privacy* erbracht.

données, *protección de datos* –, (Computer | Information | Data) Privacy, (informationelles) Persönlichkeitsrecht, (informationelle) Privatheit, (digitale) Privatsphäre, gar digitale Intimsphäre oder – obwohl scheinbar nicht in diese Reihe passend – *surveillance*. Dieses Sammelsurium an Namen, Phänomenbereichen und Erklärungstheorien hat, so unglaublich es zunächst scheinen mag, eine Unzahl von Gesetzen hervorgebracht, die jeweils einen Geltungs- und Befolgungsanspruch erheben.

Im Zentrum der Aufmerksamkeit dieser Arbeit steht der Datenschutz, die ihm zugrunde liegenden informatischen, informationswissenschaftlichen, soziologischen und rechtswissenschaftlichen Konzepte, seine rechtliche Implementation in Form des – vorwiegend deutschen, aber auch des davon abgeleiteten europäischen – Datenschutzrechts sowie – dem Primat des Rechts folgend – seine Übersetzung oder Übertragung in Organisationen, Informationsverarbeitungsprozesse und die Datenverarbeitungstechnik. Dennoch werden, weil die wissenschaftlichen Diskurse in der Informatik sehr viel weniger national oder regional beschränkt geführt werden als etwa in der Rechtswissenschaft, auch die verschiedenen *privacy*-Debatten einen breiten Raum einnehmen, da vor allem sie es sind, aus denen sich die informatischen Auseinandersetzungen zu Fragen der datenschutzfreundlichen, datenschutzfördernden und *privacy-enhancing* Technikgestaltung speisen.

Wenn Datenschutz die Lösung ist, die dann disziplinär abgebildet und beschränkt, konkretisiert und implementiert werden soll, was ist dann aber das Problem? Das Problem, zu dessen Lösung der Datenschutz angetreten ist, nenne ich vorläufig das Datenschutzproblem. Ziel der vorliegenden Arbeit ist es, die historische Konstruktion des Datenschutzproblems, des Datenschutzes als seiner (abstrakten) Lösung sowie die Architektur seiner rechtlichen Implementation aufzudecken und einer kritischen Revision zu unterziehen, um daraus Folgerungen für die Technikgestaltung zu ziehen. Die Arbeit will dabei aufdecken, welches Verständnis vom Menschen und von der Welt, von Organisationen und von der Informationstechnik, von der Informationsverarbeitung und der Informationsgesellschaft, welche Denkschulen und Theoriegebäude und welche wissenschaftlichen und vorwissenschaftlichen Annahmen und Prämissen der Analyse des Datenschutzproblems zugrunde liegen und wie sie darüber hinaus die spezifische Lösung des Datenschutzproblems – den Datenschutz – gespeist haben. Aus diesen heraus sollen nachfolgend die spezifischen architektonischen Bedingtheiten des Datenschutzrechts, das selbst dabei nur eine aller möglichen Implementationen ist, dargestellt und erklärt werden. Sowohl die der Analyse zugrunde liegenden Konzepte als auch die spezifische Operationalisierung der Lösung sollen dabei einer informatisch fundierten Kritik unterzogen werden. Abschließend sind dann die Ziele zu identifizieren, an denen sich Anforderungen an die Gestaltung datenschutzfreundlicher – und dabei nicht notwendig nur datenschutzrechtskonformer – Technik auszurichten haben, sowohl hinsichtlich der zu erreichenden Ergebnisse als auch der Verfahren.

Das klassische Vorgehen wäre, die Arbeit anhand dieser kurzen Darstellung der Ableitung von Gestaltungsanforderungen aus der Konstruktion des Datenschutzproblems aufzubauen und dabei die einzelnen Aspekte dieser Ableitung mit Quellen zu belegen. Allein, mit diesem Vorgehen lässt sich nicht belegen, dass das Datenschutzproblem, der Datenschutz, das Datenschutzrecht sowie die Gestaltungsanforderungen an Datenverarbeitungstechnik tatsächlich in der beschriebenen Art konstruiert wurden oder daraus abgeleitet werden können. Der Grund dafür liegt vor allem in der ideologischen Überladung der Debatten um *privacy*, Privatsphäre, *surveillance* und Datenschutz sowie in der Spezifik der Dogmatik in der deutschen Rechtswissenschaft, die – sowohl jeweils für sich, aber auch zusammen – derart viele verschiedene normative Konstruktionen dieser Konzepte hervorgebracht und mit Quellen belegt haben, dass sich schlicht

für jede beliebige historische Nachzeichnung der Konstruktion ein konsistentes und quellengestütztes Narrativ formulieren lässt. Es kann nicht einmal ausgeschlossen werden, dass sich nicht auch Belege finden ließen, um glaubhaft darstellen zu können, der Datenschutz sei ursprünglich geschaffen worden, um deutsche Kühe vor der Entführung durch Außerirdische zu schützen![2] Wenn sich jedoch alles, also auch das Gegenteil dessen, „beweisen" lässt, dann lässt sich nichts beweisen – jedenfalls nicht, wenn Wissenschaft mit ihrer Leitdifferenz „wahr"/„falsch" ernsthaft betrieben werden will.

Es bleibt also nur, die Entwicklung der wissenschaftlichen Diskussion und der dabei erfolgten Beschreibung, Erklärung und „Lösung" des Datenschutzproblems selbst historisch – in Form einer historischen Systemanalyse – aufzuarbeiten.

Dabei kann nur wenig auf wissenschaftliche Vorarbeiten zurückgegriffen werden. Fast alle Arbeiten – insbesondere die rechtswissenschaftlichen –, welche die Geschichte des Datenschutzes und der Datenschutzdebatten[3] darstellen, beschränken sich auf eine Ereignisdarstellung als eine Abfolge von Text- und Urteilsproduktionen und mehr oder weniger aufeinander bezogenen Debattenbeiträgen. Nur selten wird dargestellt, welche (theoretischen) Annahmen zur gesellschaftlichen Informationsverarbeitung und ihren Bedingungen getroffen wurden, welche technik-, organisations- und sozialwissenschaftlichen Theorien der Beschreibung und Erklärung des Datenschutzproblems zu Grunde gelegt wurden,[4] welche Schlussfolgerungen daraus für die abstrakte Lösung – die Lösungsarchitektur – des Datenschutzproblems gezogen und unter welchen Bedingungen welche Entscheidungen über konkrete – vor allem rechtliche – Implementationsfragen getroffen wurden und welche Aspekte, die für die Informatik und insbesondere die Technikgestaltung relevant waren oder sind, dabei unter den Tisch fallen gelassen wurden. Die meisten Arbeiten setzen schlicht das Bedürfnis, das Interesse oder das Recht auf *privacy*, Privatsphäre oder Datenschutz als – teilweise ahistorisch – gegeben voraus. Werden doch einmal Einordnungen in größere Theoriezusammenhänge vorgenommen, erschöpfen sich die Arbeiten oft in der Nutzung der ideologischen Überbaukonstruktionen für die Abwägung mit konfligierenden Interessen oder Rechten oder für den Vergleich zwischen verschiedenen Theorieansätzen, etwa „liberalen" und „kommunitaristischen". Und selbst wenn Arbeiten behaupten, dass sie tatsächlich eine historische Re-Konstruktion vornehmen würden, gibt es allzuoft große Zweifel an der wissenschaftlichen Qualität, etwa wenn als Ausgangspunkt der Analyse das Jahr 1980 – das Jahr, in dem die OECD Privacy Guidelines beschlossen wurden – gesetzt wird, also zehn Jahre nach den ersten beiden (modernen) Datenschutz- und *privacy*-Gesetzen, dem Hessischen Landesdatenschutzgesetz und dem Fair Credit Reporting Act, die beide 1970 beschlossen wurden.

Die Arbeit ist dabei wie folgt gegliedert:

Kapitel 2, *Die Geschichte des Datenschutzes*, S. 9 ff., enthält eine historische Systemanalyse der wissenschaftlichen Auseinandersetzungen zur Beschreibung, Einordnung und Begründung des Datenschutzproblems, der Ableitung des Datenschutzes als (abstrakter) Lösung aus dem Datenschutzproblem, seiner Operationalisierung und seiner Implementation im Datenschutzrecht

[2] Den Hinweis, dass dies hier nur billige und im übrigen unverständliche Polemik sei, verdanke ich Michael Plöse. Dank sei ihm auch für seinen Hinweis auf die Verbindung zur seit dem BND-Skandal diskutierten Weltraum-Theorie, deren Einbringung in die Debatte diese Polemik längst nicht mehr billig erscheinen lässt.

[3] Selbiges gilt natürlich auch für *privacy*, Privatsphäre und *surveillance* und die *privacy*-, Privatsphäre- und *surveillance*-Debatten.

[4] So kritisch schon Leib (1985), aber im Grunde folgenlos.

sowie der parallel geführten Debatten um eine für den Datenschutz geeignete und angemessene Technikgestaltung.[5]

In Kapitel 3, *Die Welt des Datenschutzes*, S. 235 ff., wird die Re-Konstruktion des Datenschutzes in seiner Ableitungskette – zugrunde gelegte Annahmen über die (organisierte) gesellschaftliche Informationsverarbeitung in der Informationsgesellschaft, Analyse der davon erzeugten oder daraus entstehenden individuellen und gesellschaftlichen Probleme sowie Lösungsarchitektur – kompakt und zusammenhängend dargestellt und einer informatisch fundierten Kritik unterzogen. Anschließend wird der Datenschutz auf der Basis eines dem Stand der wissenschaftlichen Debatte entsprechenden Angreifermodells und eines daraus abgeleiteten Bedrohungsmodells rekonzeptionalisiert und mit einem neuen Operationalisierungs- und Regelungsansatz versehen. Abschließend wird das für die Technikgestaltung relevante Verhältnis zwischen dem rekonzeptionalisierten Datenschutz und dem geltenden Datenschutzrecht bestimmt werden, unter anderem im Hinblick auf den Geltungsbereich, den verwendeten Informationsbegriff und das Prozessmodell der Informationsverarbeitung.

In Kapitel 4, *Die Technik des Datenschutzes*, S. 281 ff., werden daraus Folgerungen für die Gestaltung datenschutzfreundlicher – und dabei nicht notwendig nur datenschutzrechtskonformer – Datenverarbeitungstechnik gezogen, einerseits im Hinblick auf Anforderungen an die Gestaltung der Technikentwicklungsprozesse, andererseits in Bezug auf konkrete Gestaltungsziele.

Kapitel 5, *Zusammenfassung und Abschluss*, S. 289 ff., schließt die Arbeit mit einer Zusammenfassung der zentralen Erkenntnisse und einer Übersicht über offene Forschungsfragen ab.

Für die Arbeit werden nur drei Annahmen getroffen: Erstens wird grundsätzlich davon ausgegangen, dass die zitierten Autorinnen in ihren jeweiligen Disziplinen kompetent sind, jedoch gleichwohl disziplinär beschränkt. Zweitens wird ebenso grundsätzlich davon ausgegangen, dass Lücken in ihren Erklärungen und fehlende Explizierungen der von ihnen getroffenen Annahmen unter Nutzung der zur jeweiligen Zeit am wenigsten begründungsbedürftigen Theoriestücke gefüllt werden bzw. ergänzt werden können. Und drittens wird davon ausgegangen, dass es tatsächlich ein gesellschaftliches Problem gibt – und nicht nur ein Phantasma –, das Problem, von dem die Datenschutzdebatte, die hier analysiert wird, behauptet, es sei das Datenschutzproblem.

Die Arbeit ist keine ausschließlich informatische. Die Informatik hat sich zu großen Teilen darin eingerichtet, nur die Dimensionen und Aspekte des Datenschutzes zu sehen, die konzeptionell und instrumentell mit den Werkzeugen der (Kern-)Informatik bearbeitet werden können.[6] Sie ist damit jedoch noch nicht einmal in der Lage, das Datenschutzproblem holistisch – also in und mit seinen gesellschaftlichen, ökonomischen, rechtlichen und technischen Dimensionen und Aspekten – zu analysieren, geschweige denn kann sie begründen, warum die Lösungen des Datenschutzproblems im (kern-)informatischen Sinne, die sie als Disziplin präsentiert, auch geeignete Lösungen des Datenschutzproblems im weiteren Sinne sein sollen. Die vorliegende Arbeit *will* daher auch keine ausschließlich informatische Arbeit sein. Wissenschaftlich erscheint ein solch beschränktes und selbstbeschränkendes Vorgehen mehr als nur ungeeignet und vor dem Hintergrund der Verantwortung der Wissenschaftlerinnen gegenüber der Gesellschaft auch als nicht angemessen für einen Beitrag zur Analyse des Datenschutzproblems und zur Präsentation möglicher Lösungsansätze. Die Arbeit wird sich daher nicht nur auf informatische und informationswissenschaftliche,

[5] Im Foucaultschen Sinne könnte auch von einer Archäologie gesprochen werden, siehe Foucault (1973), allerdings nicht mit dem Ziel der Analyse des Diskurses als Diskurs, sondern mit dem Ziel der Analyse seiner Produkte: dem Datenschutzproblem, dem Datenschutz und dem Datenschutzrecht.

[6] Auf die Gefahr dieser Selbstisolierung wissenschaftlicher Disziplinen gegen gesellschaftlich relevante Probleme weist schon Kuhn (1996, S. 37) hin.

sondern auch auf sozialwissenschaftliche, insbesondere soziologische, und rechtswissenschaftliche Theorien stützen.[7]

Die mit diesem Vorgehen erzeugten Probleme dürfen allerdings nicht übersehen werden: „Die *Pfadabhängigkeit* der Analyse produziert Unterschiede, die Unterschiede machen.“[8] Diese Probleme lassen sich allerdings auch nicht einfach umgehen, denn „an explorer can never know what he is exploring until it has been explored.“[9] Gleichwohl versucht diese Arbeit, solche Defizite mit Hilfe einer historischen Systemanalyse, die zugleich ein wenig an eine *histoire globale*[10] angelehnt ist, zu minimieren: Insoweit gerade auch Recht immer nur gesellschaftlich konstruiert ist,[11] lässt sich – so die begründete Erwartung – die historisch von der Rechtswissenschaft dominierte Auseinandersetzung zur Beschreibung, Einordnung, Begründung und „Lösung“ des Datenschutzproblems mit dieser Methode *re*-konstruieren, ohne dabei dieser (vergangenen) Auseinandersetzung ein nachträglich konstruiertes Narrativ zu oktroyieren.

Als historische Systemanalyse soll dabei eine Systemanalyse verstanden werden, die einen historischen Prozess und seine Ergebnisse als System betrachtet. In klassisch konstruktivistischer Weise werden die Gesellschaft, die gesellschaftlichen Verhältnisse und die gesellschaftlichen Praktiken als real existierend betrachtet, die jedoch ausschließlich durch die Brille konkreter Disziplinen, Theorien und Schulen wahrgenommen, abgebildet und analysiert werden können,[12] indem sie im betrachtenden System als Modell *konstruiert* werden.[13] Daraus folgt, dass das betrachtete System und das im betrachtenden System kreierte Modell davon nicht gleich sind.[14] Eines der Ziele dieser Arbeit ist es demnach zu explizieren, welches Modell der Welt der Analyse des Datenschutzproblems zugrunde gelegt wurde und wird. Unter einem Problem soll dabei grundsätzlich die Differenz zwischen Sein und Sollen verstanden werden, wobei nicht nur das Sein – oder besser: das Modell des Seins –, sondern auch das Sollen konstruiert ist – von verschiedenen Akteurinnen mit ihren jeweiligen disziplinären, gesellschaftlichen, ökonomischen, kulturellen, politischen und historischen Hintergründen, eingebracht in gesellschaftliche Debatten und dort gesellschaftlich ausgehandelt, verregelt und institutionalisiert. Die Explikation des Sollens, an dem die gesellschaftlichen Informationsverarbeitungspraktiken gemessen werden, ist ein weiteres Ziel der Arbeit. Auch das Problem als Differenz zwischen Sein und Sollen ist nicht objektiv, sondern wird von den Beobachterinnen konstruiert. Und insoweit die Problemlösung zur Lösung dieses konstruierten Problems selbst wiederum konstruiert wird, ist auch sie bedingt durch das Problem[15] und die Eigenschaften der Beobachterinnen. Eine besondere Herausforderung für die Analyse des hier betrachteten Systems stellt das Aufeinandertreffen der Disziplinen dar: Die gesellschaftliche Realität der gesellschaftlichen Informationsverarbeitung unter Nutzung von Informatiksystemen in einer weitgehend verrechtlichten Informationsgesellschaft erforderte und erfordert eine dezidiert interdisziplinäre Theorie für ihre Beschreibung und Analyse, für die Beschreibung und

[7] Andererseits wird gerade dadurch die Arbeit auch erst zu einer informatischen Arbeit im Coyschen Sinne, siehe Coy (1992). Siehe dazu auch Steinmüller (1993, S. 697), der den Themenbereich der Informatik zuweist, weil er „sachlich zur Informatik gehör[t]“.

[8] Drepper (2003, S. 23 f.), oder modelltheoretisch: „das Ausgangsmodell schafft das Raster für die Problemwahrnehmung und selektiert mögliche Problemlösungen“, siehe Burkert (1984, S. 184).

[9] Bateson (1987, S. 2).

[10] Siehe Braudel (1972) und Braudel (1973).

[11] Für das Konstrukt der „herrschenden Meinung“ sehr eindrucksvoll und zugleich sehr amüsant Wesel (1979).

[12] Siehe Albert Einsteins Diktum, dass die Theorie bestimme, was wir beobachten können.

[13] Siehe Heylighen und Joslyn (2001, S. 21).

[14] Siehe dazu Alfred Korzybskis Diktum, dass die Karte nicht das Gelände sei.

[15] „The threats are what determines the policy, and the policy is what determines the design“, so Schneier (2000, S. 227) zur vergleichbaren Situation im Bereich der IT-Sicherheit.

Analyse des dabei aufgeworfenen Datenschutzproblems und für die Entwicklung und Modellierung einer geeigneten und gesellschaftlich akzeptablen Lösung, die jeweilige Umsetzung jedoch – vor allem die im Datenschutzrecht – war und ist das Ergebnis einer monodisziplinären Abbildung unter Verzerrung oder gar Auslassung der durch die Rechtswissenschaft und im Recht nicht abbildbaren Anteile – und dazu gehören eben insbesondere auch die informatischen. In der wissenschaftlichen Auseinandersetzung wird dieses Problem bislang standhaft ignoriert.[16] Die vorliegende Arbeit versucht hingegen, einen Beitrag zur Aufdeckung dieser Verzerrungen und Auslassungen zu leisten. Aus dieser Analyse sollen Folgerungen für die Gestaltung datenschutzfreundlicher – und dabei nicht notwendig nur datenschutzrechtskonformer – Informatiksysteme gezogen und begründet werden.

Kenntnisse über die Geschichte der Informatik und der Entwicklung von Informatiksystemen werden vorausgesetzt.

Im Text wird aus Gründen der besseren Lesbarkeit ausschließlich die weibliche Form benutzt. Damit sind selbstverständlich auch alle anders positionierten Menschen eingeschlossen. Ausnahmen werden nur dort gemacht, wo nachweisbar ausschließlich über Männer geschrieben oder wörtlich zitiert wird.

[16] Daraus erklärt sich wohl auch die in der deutschen Rechtswissenschaft endemische Gleichsetzung von Datenschutz und Datenschutzrecht.

2 Die Geschichte des Datenschutzes

Weder die Geschichte des Datenschutzes noch die des Datenschutzrechts beginnen Ende der sechziger Jahre in den USA[1] oder 1970 in Hessen mit der Verabschiedung des weltweit ersten so bezeichneten Datenschutzgesetzes.[2] Sie beginnt auch nicht mit der berühmten Arbeit von Samuel D. Warren und Louis D. Brandeis aus dem Jahre 1890,[3] auf die die meisten US-Autorinnen verweisen.[4] Die Geschichte des Datenschutzes und seiner rechtlichen Regulierung beginnt sehr viel früher, „[s]ie ist nur noch nicht geschrieben."[5] Und über den Ursprung des Begriffs „Datenschutz" ist nur bekannt, dass er unbekannt ist[6] – er taucht zum ersten Mal im Rahmen der Vorarbeiten zum Hessischen Datenschutzgesetz auf.[7]

Als die moderne Debatte zur *information privacy* und zum Datenschutz begann, waren die Rechtssysteme, die hier von Belang sein sollen – das der USA und das der BRD – und in welche die beiden Topoi eingefügt werden sollten, bereits hochgradig ausdifferenziert. Jede rechtliche Regelung musste sich in die bestehenden Strukturen – zumindest weitgehend – einpassen und stand dabei unter einem besonderen (gesellschaftlichen, politischen, wissenschaftlichen und insbesondere rechtswissenschaftlichen) Rechtfertigungsdruck, der zu einer ausführlichen Auseinandersetzung mit den Hintergründen, Bedingungen, Zielen und Prinzipien des Datenschutzes geführt und – wenn auch teilweise nur mittelbar, etwa über die Auslegung – das Datenschutzrecht stark beeinflusst hat. Gleichzeitig gab es dem aufkommenden Datenschutzrecht die Möglichkeit, auf vielfältige Erfahrungen aus der Rechtsgeschichte der bürgerlichen Staaten zurückzugreifen und dabei jeweils die am besten passenden Strukturelemente zu übernehmen, unpassende zu ignorieren. Die Entwicklung des modernen Datenschutzrechts ist daher nur zu verstehen, wenn sie vor dem Hintergrund der damals bestehenden gesetzlichen Regelungen, ihrer Strukturen, ihrer historischen Entwicklung und des Standes der rechtswissenschaftlichen Debatte[8] als Menge und Abfolge von Entscheidungen über Inklusion und Exklusion existierender rechtlicher Ansätze betrachtet wird. Und obwohl es sich weder beim US-amerikanischen *privacy law* noch beim deutschen Datenschutzrecht um Technikrecht[9] handelt, ist die Technikentwicklung – insbesondere der Technik zur Unterstützung von Informationsverarbeitungprozessen – wesentlicher Motor der Entwicklung und Weiterentwicklung des Datenschutzrechts gewesen.

[1] So aber etwa Tinnefeld et al. (2005, S. 79 ff.).
[2] Das behauptet aber z. B. Simitis (Simitis in: 2011, Einleitung, Rn. 1).
[3] Warren und Brandeis (1890).
[4] Siehe etwa Solove (2009, S. 15).
[5] von Lewinski (2009, S. 196).
[6] Siehe von Lewinski (2014, S. 3).
[7] Statt vieler Simitis (Simitis in: 2011, Einleitung, Rn. 2 und Fn. 9).
[8] Damit ist die Debatte etwa zum Recht in der modernen, westlichen Industriegesellschaft, zum Verhältnis von Recht und Technik, zum Verhältnis von öffentlichem und Privatrecht oder zu rechtsdogmatischen Fragen des Verfassungsrechts gemeint. Die vorfindliche Verrechtlichung lässt sich in Anlehnung an Brinckmann und Kuhlmann beschreiben als ein zum Programm geronnenes, in Rechtskonzepte verarbeitetes und in Recht implementiertes, also mehrfach modifiziertes gesellschaftliches Problem und zugleich als ein Versuch, durch Verrechtlichung dieses Problem zu beseitigen, siehe Brinckmann und Kuhlmann (1990, S. 32).
[9] Für einen Überblick über Geschichte und Inhalt des Technikrechts siehe Vec (2011).

2.1 Vorgeschichte des Datenschutzes

2.1.1 Geheimnisschutz

Eine der ältesten „rechtlichen“ Regelungen, in deren Tradition das Datenschutzrecht oft gestellt wird, ist der Teil des Eides des Hippokrates, mit dem die ärztliche Schweigepflicht begründet wurde.[10] Eigentlich in erster Linie eine Frühform der Sozialversicherung auf Gegenseitigkeit innerhalb der Ärzteschaft des alten Griechenlands, formuliert der Eid auch erstmals Grundlagen einer ärztlichen Ethik. Als Mittel zur Abgrenzung von „Nicht-Ärztinnen“ – Kurpfuschern, Scharlatanen, Quacksalbern, Hexen, Heilerinnen, Badern, Chirurgen[11] – geht es im Kern um einen Strukturschutz, einen Schutz der Ärzteschaft – später auch der Ärztinnenschaft – selbst sowie ihres „guten Rufes“. Der Schutz der Patientinnen ist dem Strukturschutz demgegenüber unter- und nachgeordnet.

Auch beim Beichtgeheimnis, das auf dem Vierten Laterankonzil 1215 formuliert wurde, handelt es sich in erster Linie um einen Strukturschutz, während der Schutz des Individuums nur nachrangig war. Das Beichtgeheimnis schützte vor allem die Kirche, weil es bei der Durchsetzung der gleichzeitig beschlossenen Pflicht zur Beichte half. Warum es überhaupt notwendig wurde, den Beichtenden Geheimhaltung zu gewährleisten, lässt sich im Gegensatz zum alten Griechenland nicht damit erklären, dass es eine Trennung zwischen einer Sphäre der Öffentlichkeit und einer der Privatheit gab, wie dies für moderne Gesellschaften typisch ist, weil das Mittelalter von Gemeinschaften geprägt war.[12]

Das Bankgeheimnis lässt sich historisch bis zur Gründungszeit der ersten großen Staatsbanken Ende des 16. Jahrhunderts zurückverfolgen, in Deutschland bis 1619, als Verschwiegenheitspflichten für Bankmitarbeiter in Hamburg und Nürnberg statuiert wurden.[13] Mit dem Bankgeheimnis wurden dabei sowohl die Interessen der Kundinnen als auch die der Bank geschützt, wobei gerade „die kleinen Angestellten der Bank als Normadressaten besonders in die Pflicht genommen wurden.“[14]

In der liberalistischen Geschichtsschreibung werden die genannten Geheimschutzregelungen nicht als Ergebnisse von Strukturschutzentscheidungen betrachtet, sondern einer vor allem in Frankreich entwickelten Theorie folgend als vertraglicher oder vorvertraglicher Schutz anvertrauter Geheimnisse, neben denen sich jedoch „schon früh“ auch ein Schutz gegen „bestimmte [...] Indiskretionen [...] außerhalb besonderer Vertrauensverhältnisse“ entwickelt habe, namentlich die *actio iniuriarum* des klassischen römischen Rechts.[15]

Das Postgeheimnis, zu dessen Einhaltung sich der römisch-deutsche König und spätere Kaiser Josef I. 1690 verpflichtete, begünstigte hingegen nicht etwa die einzelnen Postbenutzerinnen, sondern schützte ursprünglich nur die deutschen Territorialfürsten als Obrigkeiten vor Übergriffen der Reichsgewalt. Erst die Preußische Postordnung von 1712 gewährte auch der allgemeinen Bevölkerung Schutz.[16]

Auch das Steuergeheimnis und das Statistikgeheimnis dienen vor allem dem Schutz der Struktur, in beiden Fällen also den Interessen des Staates. Ersteres soll „die Steuerpflichtigen zur

[10] Siehe etwa Tinnefeld et al. (2005, S. 179).
[11] Die Chirurgen wurden erst nach dem Dreißigjährigen Krieg in die (akademische) Ärzteschaft kooptiert, vorher gehörten sie zu den Badern, einer sozial inferioren Klasse von Handwerkern.
[12] Grundlegend zur Unterscheidung von Gemeinschaft und Gesellschaft, siehe Tönnies (1887).
[13] Siehe Petersen (2005, S. 7).
[14] Petersen (2005, S. 8).
[15] Maass (1970, S. 3 ff.).
[16] Siehe Austermühle (2002, S. 60 f.).

Ehrlichkeit gegenüber dem Finanzamt anhalten“[17] und letzteres zur Ehrlichkeit gegenüber Statistikämtern. In beiden Fällen werden die Mitarbeiterinnen der jeweiligen Behörden zur Verschwiegenheit gegenüber Dritten verpflichtet, nicht aber die Behörden selbst. Auch folgt aus den beiden Geheimnisarten insbesondere nicht, dass die erlangten Informationen nicht auch fundamental gegen die Interessen der Betroffenen genutzt werden können. Es ist deshalb kein Zufall, dass sowohl das Deutsche Reich als auch die BRD besonders viel Wert auf das Statistikgeheimnis legten.[18]

Als letzte wichtige Geheimhaltungspflicht sei hier das Amtsgeheimnis genannt. Bis zum Ende des 19. Jahrhunderts, in dem auch Privatgeheimnisse seinem Schutz unterworfen wurden, diente das Amtsgeheimnis allein dem Geheimhaltungsinteresse des Staates.[19]

2.1.2 Beschränkung von Datenmacht

Neben den Geheimnisschutz trat die Regulierung von Datenmacht.[20]

Die älteste Beschränkung von Datenmacht ist wohl das Verbot der Volkszählung bei den Jüdinnen, das der Talmud seit ca. 3.000 Jahren „im Sinne bewußter Begrenzung staatlicher Herrschaftsmittel“ verlangt.[21] Allgemein bekannt ist die Volkszählung in Israel, von der die biblische Weihnachtsgeschichte berichtet.

Mit der juristischen Figur des Oberaufsichtsrechts (*ius [supremae] inspectionis*) wurde die Informationsverarbeitung des Staates rechtlich eingefangen und erst auf den Staatszweck und später auf bestimmte Staatsfunktionen begrenzt.[22] Mit der Ausdifferenzierung und Spezialisierung der Verwaltung[23] wurde die Datenmacht durch Aufgaben- und Zuständigkeitsnormen weiter strukturell beschränkt. Andere Formen der Beschränkung von staatlicher Datenmacht sind explizite Löschungsvorschriften – wie das Straftilgungsgesetz vom 9. April 1920 – und Transparenzregelungen – wie die Abschaffung von Geheimprozessen im Strafrecht.

2.2 Frühgeschichte des Datenschutzes

Bis zur zweiten Hälfte des 19. Jahrhunderts gab es also fast ausschließlich objektivrechtliche Geheimhaltungsregelungen und Beschränkungen von Datenmacht. Die strukturalistischen Ansätze der Regelung von Informationsverhältnissen gehen den individualistischen Konzeptionen somit zeitlich voraus, auch wenn sie in der heutigen Debatte „fast vollständig durch eine subjektive, schutzrechtliche Perspektive verdrängt“ wurden.[24]

[17] Däubler et al. (2010, Einleitung, Rn. 41).

[18] Sowohl bei der Volkszählung 1939 als auch bei der geplanten Volkszählung 1983 diente das Statistikgeheimnis einzig der Bekämpfung des Misstrauens in der Bevölkerung, siehe Aly und Roth (1984, S. 24) und Steinmüller (2007, S. 160). Sowohl Götz Aly und Karl Heinz Roth als auch Wilhelm Steinmüller zeigen auch die anderen Kontinuitäten zwischen den beiden Volkszählungen auf.

[19] von Lewinski (2009, S. 208 ff.).

[20] Als Datenmacht bezeichnet Kai von Lewinski das Informationsgefälle zwischen einer Organisation und einem Individuum, siehe von Lewinski (2009, S. 200). Angemessener scheint der Begriff Informationsmacht, siehe Tinnefeld et al. (2005, S. 1). Strukturell den gleichen Streit gab es schon bei der Frage „Datenschutz oder Informationsschutz?“, siehe Steinmüller (1970, S. 87). Gerade wegen der Verbindung zum Datenschutz wird im Folgenden aber weiter Datenmacht benutzt.

[21] Aly und Roth (1984, S. 82).

[22] Dazu und zum folgenden von Lewinski (2009, S. 204 ff.).

[23] Weber (1995, S. 238 ff.).

[24] von Lewinski (2009, S. 212).

2.2.1 Persönlichkeitsrecht und *right to privacy*

Der bürgerliche Liberalismus stellt das Individuum und seine Interessen in den Mittelpunkt der Aufmerksamkeit. Einer der Ausflüsse davon ist das allgemeine Persönlichkeitsrecht, das heute sowohl in der Privatrechtsordnung als auch verfassungsrechtlich – Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz – einen sehr weit gehenden Schutz genießt und das in einer seiner Ausprägungen als Recht auf informationelle Selbstbestimmung grundrechtlicher Anknüpfungspunkt des Datenschutzrechts ist.

Einer der ersten wichtigen Vertreter bei der Entwicklung des Persönlichkeitsrechts war Josef Kohler.[25] In Abgrenzung zu einem reinen Verwertungsrecht, wie es auch das *copyright* sehr lange ausschließlich war, vertrat Kohler die Ansicht, dass es ein grundlegendes „Individualrecht" gebe und dass schon aus diesem folge, „daß ein Jeder alleiniger Herr ist, zu bestimmen, welche Aeußerungen und Kundgebungen er in das Publikum tragen will und welche nicht; auch das ist ein Individualrecht, denn nur dem Autor steht die Bestimmung darüber zu, ob er die Aktion an das Publikum bewirken will, oder nicht".[26] Dieses umfassende Individualrecht gebe es schon im alten römischen Recht als *actio iniuriarum*, sei aber später immer nur einschränkend – und verfehlt – als Ehrschutz verstanden worden.[27] „Die[] actio injuriarum aber ist nicht ein aus der Luft gegriffenes Sonderwesen, sie ist vielmehr die ganz entsprechende Reaktion gegen den unbefugten Eingriff in das Recht der alleinigen Selbstbestimmung über das Auftreten an die Oeffentlichkeit."[28] Das Konzept des Individualrechts übernimmt Otto von Gierke.[29] Er ist es jedoch, der diesem Recht die bis heute gebräuchliche Bezeichnung „Persönlichkeitsrecht" gibt: „»Persönlichkeitsrechte« nennen wir Rechte, die ihrem Subjekte die Herrschaft über einen Bestandtheil der eigenen Persönlichkeitssphäre gewährleisten."[30]

[25] Hierzu und zum folgenden siehe Kohler (1880).
[26] Kohler (1880, S. 137).
[27] Siehe Kohler (1880, S. 130).
[28] Kohler (1880, S. 158 f., Fn. 1).
[29] Siehe von Gierke (1895).
[30] von Gierke (1895, S. 702). Auch sonst sind die Ausführungen sehr modern und entsprechend weitgehend der heute vertretenen Meinung: „Im deutschen und modernen Recht dagegen sind zahlreiche Typen von Rechten an der eignen Person zu selbständiger Ausgestaltung gelangt. Manche von ihnen sind durch die neuere Gesetzgebung in ihrem Sonderdasein so befestigt, dafs sie sich von dem allgemeinen Rechte der Persönlichkeit nicht minder scharf abheben, als das Eigenthum oder die väterliche Gewalt. Die Persönlichkeitsrechte müssen daher auch begrifflich heute als eine eigene Kategorie der besonderen Rechte anerkannt werden und fordern gebieterisch die ihnen gebührende Stelle im System.

Vieles freilich ist hier noch im Werden. Darum sind die Grenzen zwischen den besonderen Persönlichkeitsrechten und dem allgemeinen Rechte der Persönlichkeit zum Theil fliefsend und unsicher.[Fußnote 8: Manche Bestandtheile der Privatrechtssphäre sind durch besondere öffentlichrechtliche Garantien in bestimmter Richtung als selbständige Rechte abgehegt, ohne dafs hiermit zugleich für die Privatrechtsordnung ihre Ausscheidung aus dem allgemeinen Rechte der Persönlichkeit geboten wäre. Dies gilt z. B. von den Rechten auf gewisse durch einen besonderen Strafrechtsschutz gesicherte Persönlichkeitsgüter, wie Hausfriede, Brief- und Schriftengeheimnifs, Gräberruhe, religiöses Gefühl, Rechtsfriede [...]. Es gilt ferner von zahlreichen den Individuen durch das Verfassungsrecht als Grundrechte zugesicherten Rechten auf eine bestimmte Art der freien Bethätigung der Persönlichkeit, wie Gewissensfreiheit, Recht der freien Meinungsäufserung, Lehr- und Unterrichtsfreiheit, Vereins- und Versammlungsfreiheit, Freizügigkeit, etwa auch Verehelichungsfreiheit, Erwerb von Grundeigenthum u. s. w.] Jedesfalls erschöpfen die in feste gesetzliche Form gegossenen Persönlichkeitsrechte nicht den an sich hierfür geeigneten Stoff. Vielmehr lassen sie empfindliche Lücken. Zur Ausfüllung solcher Lücken mufs da, wo das Rechtsbewufstsein der Gegenwart dies heischt, auf das allgemeine Recht der Persönlichkeit zurückgegriffen werden, bis aus ihm ein neues besonderes Recht herausgeholt ist." von Gierke (1895, S. 704 f.).

Wichtiger noch ist Kohler allerdings als Ideengeber für einen anderen grundlegenden Text der Datenschutzrechtsgeschichte. Hans-Heinrich Maass ist der erste, der darauf hinweist, dass die zehn Jahre danach erschienene Schrift von Samuel D. Warren und Louis D. Brandeis inhaltlich mit dessen Ausführungen „weitgehend überein[stimme].“[31] Kohler werde zwar nicht zitiert, aber Brandeis dürfte die deutsche Rechtsliteratur gekannt haben, vielleicht sogar Kohlers Arbeit selbst.[32] Es gibt große Übereinstimmungen in der Argumentationsstruktur, bei der ungewöhnlichen – und damals nicht mehrheitsfähigen – Auslegung des Inhalts der *actio iniuriarum*, bei einigen Zitaten[33] und bei der Wortwahl. Während Kohler aus der Sicht der Autorinnen schreibt, fordern Warren und Brandeis[34] ein „right to privacy“ aus der Sicht der Betroffenen, über die geschrieben wird. Vor dem Hintergrund damals neuer technischer und daraus folgender gesellschaftlicher Entwicklungen (Instantanphotographie, Telegraphie, Boulevardpresse) zeigen die Autoren auf, dass die traditionellen Mechanismen zum Umgang mit den daraus erwachsenden Gefahren für das Individuum nicht mehr erfolgversprechend seien: Vor der Erfindung der Sofortbildkamera lagen die Belichtungszeiten teilweise bei mehreren Minuten, jedenfalls waren sie aber so lang, dass die Photographierten nicht nur einwilligen mussten, sie mussten vielmehr sogar aktiv mitwirken und stillstehen oder stillsitzen.[35] Die Telegraphie hingegen ermöglichte die weiträumige Verbreitung vorher nur lokal bekannter Nachrichten, während die Boulevardpresse vor allem der Verbreitung von „gossip“[36] dient. Weil Warren und Brandeis nicht einfach schreiben konnten, dass die Privatpartys eines Bostoner It-Girls – Warrens Frau – von der Boulevardpresse nur soweit und in der Form der Öffentlichkeit zugänglich gemacht werden sollten, wie es die Veranstalterin wünschte – das wäre genauso unbürgerlich unhöflich gewesen wie der „gossip“ der Medien –, verwiesen sie auf ein höherwertiges „right to be let alone“.[37] Warren und Brandeis weisen dabei explizit darauf hin, dass zwar in der Vergangenheit das „right to privacy“ oftmals vermittelt über das Eigentum geschützt wurde, dieses Recht sich aber nicht in einem Eigentumsrecht erschöpfe.[38] Inhaltlich werde dem Individuum das Recht gewährt „of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.“[39] Die wichtigsten Möglichkeiten zur Einschränkung des *right to privacy* seien ein überwiegendes öffentliches Interesse[40] und die Einwilligung der Betroffenen.[41]

Sowohl Kohler als auch Warren und Brandeis betrachten eine Anwendungsdomäne, in der es strukturell eine klare Trennung zwischen privat und öffentlich gibt: Der Akt des Veröffentlichens – entweder durch die Autorin (bei Kohler) oder über die Betroffenen (bei Warren und Brandeis) – im Sinne eines Sich-Wendens an eine unbeschränkte Öffentlichkeit konstituiert erst die beiden Sphären und macht sie klar unterscheidbar. Wo es nicht darum geht, sich an eine unbeschränkte (bürgerliche) Öffentlichkeit zu wenden, und wo nicht der Akt des Veröffentlichens das binäre

[31] Maass (1970, S. 15).
[32] Maass (1970, S. 15, Fn. 63).
[33] Zum Beispiel zitieren beide Texte das gleiche französische Pressegesetz, das *Loi Relative à la Presse* vom 11. Mai 1868. Zumindest für die US-amerikanische Rechtswissenschaft ist das mehr als ungewöhnlich.
[34] Den Text habe Brandeis, der später einer der Obersten Bundesrichter wurde, allein geschrieben, so die herrschende Meinung spätestens seit 1960, vgl. Prosser (1960, S. 384).
[35] Oder sie waren so tot wie der alte Bismarck, dann wurden gesetzliche Regelungen eingeführt, siehe Tinnefeld et al. (2012, S. 138, Fn. 487).
[36] Warren und Brandeis (1890, S. 196)
[37] Sie zitieren damit Thomas M. Cooley, während Kohler strukturell ähnliches aus der Bibel zitiert: „Noli me tangere“ – Rühre mich nicht an, siehe Kohler (1880, S. 4 und S. 303).
[38] Siehe Warren und Brandeis (1890, S. 205).
[39] Warren und Brandeis (1890, S. 198).
[40] Warren und Brandeis (1890, S. 214 ff.).
[41] Warren und Brandeis (1890, S. 218).

System Öffentlichkeit / Privatheit (besser: Nicht-Öffentlichkeit) erst schafft, lassen sich weder Kohlers noch Warrens und Brandeis' Konzepte unbesehen auf das Problem moderner Informationsverarbeitung und dessen Bedingungen anwenden. Eines der fundamentalen Probleme der Geschichte von *privacy* und Persönlichkeitsrecht besteht darin, dass es dennoch immer wieder versucht wurde.

2.2.2 Durchbrüche

Sowohl in den USA als auch in Deutschland dauerte es verhältnismäßig lange, bis sich die vorgenannten Ideen voll durchsetzten. Zwar wurden in der deutschen Geschichte immer wieder einzelne Ausprägungen des Persönlichkeitsrechts als selbständige Rechte anerkannt – wie das Recht am eigenen Bild oder das Namensrecht –, aber erst mit der „Schacht"-Entscheidung des Bundesgerichtshofes[42] von 1954 ist das allgemeine Persönlichkeitsrecht als solches im Zivilrecht anerkannt worden.[43] Die zivilrechtliche Anerkennung des „right to privacy" erfolgte sogar erst 1960.

Das allgemeine Persönlichkeitsrecht bildet ein sehr umfassendes und darum schwer zu handhabendes Konzept. Darum ist schon sehr früh nicht nur durch die Konstruktion besonderer Persönlichkeitsrechte, sondern auch durch innere Strukturierung versucht worden, den Umgang damit zu erleichtern. Die lange Zeit wirkmächtigste Konzeption stammt von Heinrich Hubmann.[44] Kern des Persönlichkeitsrechts seien die Selbstbestimmung der Person, das Recht auf Entfaltung der Persönlichkeit, das Recht an der Persönlichkeit und das Recht auf Individualität.[45] Mit der Aufteilung des Rechts auf Individualität in drei zu schützende Sphären (Individualsphäre, Privatsphäre und Geheimsphäre)[46] gilt Hubmann als Begründer der Sphärentheorie, die vom Bundesverfassungsgericht bis 1983 vertreten wurde. „Während die Persönlichkeitssphäre [...] die wertvollen Beziehungen des Menschen zur Welt erfaßt, schützt ihn die Individualsphäre in seiner Einmaligkeit und Eigenart, sie wahrt sein Eigensein in der Welt und seinen Eigenwert in der Öffentlichkeit. Privatsphäre und Geheimsphäre dagegen schützen den Menschen vor der Welt, sie hüten sein Eigenleben vor der Öffentlichkeit."[47] Zur Individualsphäre gehöre nach Hubmann der Name, die Firma und die Ehre, wobei zu letzterem auch der Kredit zähle. Die Privatsphäre umfasse „jenen Teil des Eigenlebens, der an sich offen zu Tage liegt, der für jeden ohne weiteres zugänglich ist. [...] Die Privatsphäre kann [...] ihrer Natur nach nur Schutz vor der Öffentlichkeit, nicht aber vor unmittelbarer Kenntnisnahme durch einzelne oder vor Weitergabe im engen Familien- oder Bekanntenkreis verlangen; ihr kommt kein Schutz in der Nichtöffentlichkeit zu. [...] Die Geheimsphäre umfaßt dagegen jenen Teil persönlichen Lebens, persönlichen Handelns und persönlicher Gedanken, von dem niemand oder höchstens ein genau begrenzter Kreis von Vertrauten Kenntnis nehmen soll, an dem also Geheimhaltungsinteresse besteht. Sie ist nicht nur vor der Öffentlichkeit, sondern auch vor unbefugter Kenntnisnahme durch einzelne zu sichern."[48] Die Privatsphäre biete „Schutz gegen Veröffentlichung", die Geheimsphäre „auch Schutz gegen unbefugte Kenntnisnahme".[49] Die Privatsphäre schütze auch nicht gegen private Verwertung.

[42] BGHZ 13, 334 ff. – Veröffentlichung von Briefen.
[43] Maass (1970, S. 18).
[44] Siehe Hubmann (1953).
[45] Siehe Hubmann (1953, S. 85 ff.).
[46] Siehe Hubmann (1953, S. 216 ff.).
[47] Siehe Hubmann (1953, S. 217).
[48] Siehe Hubmann (1953, S. 228).
[49] Siehe Hubmann (1953, S. 235 ff.).

Für den Durchbruch des „right to privacy“ im US-amerikanischen Zivilrecht sorgte William L. Prosser 1960.[50] Während Warren und Brandeis noch von einem alles umspannenden Konzept ausgingen – der „inviolate personality“ –, behauptet Prosser, es handele sich bei Eingriffen in das „right to privacy“ nicht um *eine* unerlaubte Handlung (*tort*), sondern um Eingriffe in vier verschiedene Interessen („four different interests“), die zwar durch einen gemeinsamen Namen (*privacy*), aber sonst durch nichts verbunden seien. Die vier Eingriffe seien: 1. „Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.“ 2. „Public disclosure of embarrassing private facts about the plaintiff.“ 3. „Publicity which places the plaintiff in a false light in the public eye.“ 4. „Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.“[51] Im ersten Fall sei das geschützte Interesse „a mental one“,[52] im zweiten und im dritten Fall jeweils die Reputation[53] und im vierten Fall ein Eigentumsrecht am eigen Namen und Aussehen.[54] Prossers vier Eingriffe hatten großen Einfluss auf das „right to privacy“ in den USA. Vor allem Gesetzgeber und Rechtsprechung benutzten sie wegen ihrer einfachen Handhabbarkeit. Gleichzeitig zerstörte Prosser damit die Entwicklungsfähigkeit des „right to privacy“, weil er es als in sich abgeschlossen präsentierte: Was sich nicht unter einen der vier Eingriffe Prossers subsumieren ließ, sollte prinzipiell kein Eingriff sein. Der zivilrechtliche Durchbruch wurde also mit gleichzeitiger Stagnation erkauft.[55]

In der rechtswissenschaftlichen Literatur wurden Prossers Ausführungen hingegen überwiegend nicht geteilt. Nicht erst mit der Betrachtung der Auswirkungen der automatisierten Informationsverarbeitung auf die *privacy*, die sich kategorial nicht mit Prossers vier Eingriffen fassen ließ und später *information privacy* genannt wurde, wurde scharfe Kritik an Prosser und seiner Argumentation geäußert. Die schärfste Kritik kam dabei unzweifelhaft von Edward J. Bloustein.[56] Er rekapituliert die Aussage von Warren und Brandeis, wonach das grundlegende Prinzip und das schützenswerte Gut die „inviolate personality“ sei und schreibt: „I take the principle of »inviolate personality« to posit the individual's independence, dignity and integrity; it defines man's essence as a unique and self-determining being.“[57] *Privacy* schütze also Würde und Selbstbestimmung. Bloustein ist wohl auch der erste, der darauf hinweist, dass es nicht nur eine allgemeine gesellschaftliche Erwartung gebe, dass „information given for one purpose will not be used for another“, sondern dies auch begrüßte.[58]

Am „Vorabend“ des Beginns der modernen Datenschutzdebatte hat Harry D. Krause das bundesdeutsche Persönlichkeitsrecht mit dem US-amerikanischen *right to privacy* verglichen. Neben vielen Gemeinsamkeiten hat er zwei Unterschiede aufgezeigt: Das Persönlichkeitsrecht ist breiter angelegt – es enthält etwa auch den Ehrschutz, während *libel* und *slander* nicht zur *privacy* gezählt werden – und es ist auf Erweiterbarkeit ausgelegt, um auf neue technische oder

[50] Prosser (1960).
[51] Prosser (1960, S. 389).
[52] Prosser (1960, S. 392).
[53] Prosser (1960, S. 398 und S. 400).
[54] Prosser (1960, S. 406).
[55] Siehe ausführlich Richards und Solove (2010).
[56] Bloustein (1964). Die Kritik ist vielfach aufgegriffen worden. Generationen von vor allem US-amerikanischen Juristinnen haben dabei sowohl Prosser als auch Bloustein zitiert, in keinem Fall allerdings unter Hinweis auf die doch sehr unverblümte Schlussfolgerung, die Bloustein zieht: Für die „Einordnung“ vieler Gerichtsurteile in die vier Klassen seiner *invasions* habe Prosser die Urteilstexte inhaltlich stark verzerrt dargestellt – sie also passend gemacht. Im Kern ist das der Vorwurf unwissenschaftlichen Arbeitens.
[57] Bloustein (1964, S. 971). Siehe vor allem den von Bloustein (1964, S. 985 f.) angesprochenen Fall *Pavesich v. England Life Insurance Co.*, in dem das Gericht „invasions of privacy“ als Versklavung markiert, sowie die umfassende Auseinandersetzung bei Allen (2012).
[58] Bloustein (1964, S. 999).

gesellschaftliche Entwicklungen reagieren zu können.[59] Eine solche vergleichende Analyse nimmt – aus europäischer Sicht, die nicht nur die BRD, sondern mehrere europäische Länder umfasst – auch Stig Strömholm vor und kommt dabei zu ähnlichen Ergebnissen.[60]

Zwar verweisen schon Kohler sowie Warren und Brandeis auf die Einwilligung als einen der wichtigsten Rechtfertigungsgründe für Eingriffe in das Persönlichkeitsrecht und die *privacy*, aber erst Oscar M. Ruebhausen und Orville G. Brim, Jr., haben – unter Rückgriff auf die Einwilligung im medizinischen Bereich – ausführlich dargestellt, welche Anforderungen an eine Einwilligung zu stellen seien, insbesondere im Hinblick auf die Notwendigkeit vorheriger, vollständiger Information der Betroffenen und die absolute Freiwilligkeit. Sie zeigen gleichzeitig, warum es im Bereich der Forschung dabei zu Problemen kommen kann: Die vorher gegebene Information kann die Antworten der Betroffenen beeinflussen und damit die Forschung unmöglich machen, und vor dem Hintergrund möglicher Wissensunterschiede zwischen Forscherinnen und Beforschten kann die Freiwilligkeit der Einwilligung fraglich werden, genauso wie beim Vorliegen sozialer Zwänge. Neben Zwecksetzung und Zweckbindung fordern Ruebhausen und Brim Aufsichtsgremien, Verfahrensregelungen und eine Selbstverpflichtung der Forscherinnen. Auch schlagen sie vor, wenn möglich nur anonyme Informationen zu erheben und zu verwenden. Sie unterscheiden sechs Anonymitätsstufen, je nachdem wie lange und wem gegenüber die Betroffenen im Zuge der Informationsverarbeitung identifizierbar bleiben. Abschließend weisen sie darauf hin, dass weder die von ihnen vorgeschlagenen Prinzipien noch irgendwelche anderen in der Lage seien, den zugrunde liegenden gesellschaftlichen Interessengegensatz aufzulösen – es gehe immer nur darum, zwischen den Interessen eine Balance zu finden.[61]

Die Debatte um das Persönlichkeitsrecht und die *privacy* wurde nicht nur innerhalb der Wissenschaften geführt, sondern auch in der Gesellschaft insgesamt. Eine Vorreiterrolle nahmen dabei die USA ein.

2.2.3 Popularisierung

Während die vorherrschende ideologische Ausrichtung der US-amerikanischen Gesellschaft noch den Vorstellungen des naiven Liberalismus des 19. Jahrhunderts folgte, hatten sich die gesellschaftlichen Verhältnisse mit der durchgreifenden Industrialisierung, dem Siegeszug des Fordismus, gesteigerter Mobilität, Konsumismus und der verstärkten Urbanisierung grundlegend gewandelt. Spätestens nach dem Ende des Zweiten Weltkrieges waren die Veränderungen nicht mehr zu ignorieren. In teilweise stark reißerischen Werken wurden sie öffentlich diskutiert.

David Riesman, Nathan Glazer und Reuel Denney legten mit ihrem Werk „The Lonely Crowd“ eine der ersten soziologischen Untersuchungen des Nachkriegsamerikas und die damals meist diskutierte Charakterstudie der US-amerikanischen Gesellschaft vor dem Hintergrund zunehmender Macht staatlicher und privater Organisationen vor.[62] Sie identifizierten drei Charaktertypen: Ursprünglich habe die Gesellschaft auf einer „tradition-directed“ Kultur aufgebaut, für die überkommene Regeln konstitutiv seien. Ersetzt worden seien sie von Menschen mit einem „inner-directed“ Charakter, die nicht vorgegebenen Regeln, sondern in der Kindheit und Jugend vermittelten Werten folgten. Aus diesen verinnerlichten Werten zögen sie Selbstsicherheit und die Möglichkeit der Selbstbestimmung. Dieser Typus entspricht damit dem US-amerikanischen Selbstbild des „rugged individualism“. Im Gegensatz dazu sei die dritte Gruppe der „other-

[59] Krause (1965).
[60] Strömholm (1967).
[61] Ruebhausen und Brim (1965).
[62] Riesman et al. (1950).

directed people“, die im Zuge der Industrialisierung und der Ausbreitung der Mittelschicht entstanden sei, hochgradig flexibel und definiere sich selbst darüber, wie sie im Verhältnis zu anderen leben, wohnen, arbeiten, essen, sich kleiden oder sich verhalten würden. Sie würden also nur versuchen, den Erwartungen anderer, vor allem in ihrem Konsumverhalten, zu entsprechen. Auf diese flexiblen und konformistischen Menschen stütze sich auch die moderne Organisation. Für die liberale Gesellschaft und die *privacy* des Individuums sei das allerdings gefährlich:

> „Whereas etiquette built barriers between people, socialized exchange of consumer taste requires that privacy either be given up, or be kept, like a liberal theologian's God, in some interstices of one's nature. Before the peer-group jury there is no privilege against self-incrimination.“[63]

Die zweite wichtige Arbeit dieser Zeit, „White Collar: The American Middle Classes“ von C. Wright Mills, beschreibt das Auftauchen der Angestellten als distinkter Gruppe innerhalb der Mittelschicht und die gesellschaftlichen Auswirkungen.[64] Vor allem geht es bei Mills um die Entfremdung in der Industriegesellschaft des Spätkapitalismus.

> „Mechanized and standardized work, the decline of any chance for the employee to see and understand the whole operation, the loss of any chance, save for a very few, for private contact with those in authority—these form the model of the future.“[65]

Ein dritter Bestseller der fünfziger Jahre ist „The Organization Man“ von William Whyte.[66] Auch Whyte beschreibt die Mittelschicht als konformistisch, die sich freiwillig der Organisation unterwerfe, gleichzeitig damit aber ein „Weiter-so“ institutionalisiere. In allen drei Werken wird – unter anderem mit Verweis auf die *privacy* – die Autonomie des Individuums als bedroht beschrieben.

Neben diesen von Soziologen verfassten Werken erschienen zeitlich passend zum Beginn der „modernen“ *privacy*-Debatte Mitte der sechziger Jahre zwei populärwissenschaftliche Bücher: „The Naked Society“ von Vance Packard und „The Privacy Invaders“ von Myron Brenton.[67] Packard identifiziert die Zunahme des Organisationsbedarfes der komplexer werdenden Gesellschaft als erste treibende Kraft bei der Unterminierung der *privacy*. Zweitens bewege sich die amerikanische Gesellschaft in Richtung einer „Garrison State Mentality“, vor allem aufgrund des Kalten Krieges. Drittens sei eine Überflussgesellschaft, als die Packard die USA sieht, anfälliger für *privacy*-Verletzungen, weil es eine stärkere Notwendigkeit gibt, zur Vermarktung immer neuer Produkte möglichst viele Informationen über die Verbraucherinnen zu erheben. Viertens werde die *privacy* um so stärker gefährdet, je mehr sich die privaten Detekteien ausbreiten und damit eine Überwachungsindustrie entstehen ließen. Und fünftens sieht Packard in der technischen Entwicklung selbst eine große Gefährdung der *privacy*, den „electronic eyes, ears, and memories“. In eine ähnliche Kerbe schlägt Brenton, der auch darauf verweist, dass grundsätzlich angemessene Datenverarbeitung im Umfang so stark zunehmen könne, dass sie im Endeffekt nicht mehr angemessen sei. Außerdem gelinge es den Datenverarbeitern zunehmend, ihre eigenen Interessen vor sich selbst und vor der Öffentlichkeit als Recht zu definieren und dem Recht auf *privacy* gegenüberzustellen:

[63] Riesman et al. (1950, S. 97).
[64] Mills (1951).
[65] Mills (1951, S. 212).
[66] Whyte (1956).
[67] Packard (1964); Brenton (1964).

> The point must be conceded: there are »reasonable« encroachments on our privacy, the inevitable price we have to pay for order and progress in the confusing 1960's. *It is the thesis of this book, however, that »reasonable« encroachments are fast becoming unreasonable and irresponsible full-scale invasions, denigrating our privacy to an alarming degree and tending to make intrusion a way of every life.* Too often, these days, our »inviolate personality«, as Justice Louis Brandeis called it, is not only being violated—it is cynically being snatched from us by individuals and institutions who have kidded themselves into believing they have as much right to it as we.[68]

Brenton beschreibt zwei grundlegende Gefahren, die mit der sich entwickelnden Computertechnik einhergehen würden: Erstens die Betrachtung des Menschen ausschließlich als Nummer, als Objekt, das jedem privaten und staatlichen Informationsinteresse offensteht, zweitens die Konzentration, Verknüpfung und Entkontextualisierung personenbezogener Daten mit Hilfe von Computern.[69]

2.3 Computer, Privacy, Datenschutz

2.3.1 Die Anfänge der Debatte in den USA

In einer Phase zunehmender Liberalisierung nach der Kommunistinnenjagd der fünfziger Jahre, die besonders mit dem *House Committee on Un-American Activities* des US-Repräsentantenhauses, dem *Permanent Subcommittee on Investigations* des US-Senats und einem seiner Vorsitzenden – Joseph McCarthy – verbunden sind, fanden zwischen 1959 und 1969 mehr als zehn Hearings zu Themen rund um *privacy* und Informationsfreiheit statt, die großen Einfluss sowohl auf die öffentliche wie die wissenschaftliche Debatte hatten.[70] Die wichtigsten davon waren die Hearings im Repräsentantenhaus „Special Inquiry on Invasion of Privacy“ (1965/66) und „The Computer and the Invasion of Privacy“ (1966), sowie die Hearings im Senat „Invasion of Privacy“ (1965/66), „Right of Privacy Act of 1967“ (1967) und „Computer Privacy“ (1967).

Während ein Unterausschuss des US-Repräsentantenhauses unter der Leitung von Cornelius Gallagher eine Anhörung über den Einsatz von Persönlichkeitstest in Arbeitsverhältnissen und deren Auswirkungen auf die *privacy* durchführte – die „Special Inquiry on Invasion of Privacy“ –, kam ein Report über Vorschläge für die Einrichtung eines „National Data Center“ an die Öffentlichkeit. Obwohl es in dem Report vor allem um eine Darstellung der Vor- und Nachteile zentralisierter statistischer Datensammlungen ging, wobei mögliche Gefahren für die *privacy* ignoriert wurden, wurde er in der Öffentlichkeit als Vorschlag für eine zentrale Sammlung aller Informationen, die in US-amerikanischen Bundesbehörden anfallen, und deren Weitergabe an öffentliche und private Stellen wahrgenommen und heftig kritisiert.[71] Während der Autor dieses Reports, Edgar Dunn, jr., darauf verweist, dass es ausschließlich darum gehe, ein „*statistical* information system“ aufzubauen, und solche Systeme deutlich von „*intelligence* systems“ abgegrenzt wissen will,[72] macht Arthur Miller deutlich, dass vor dem Hintergrund der damals aktuellen und absehbaren Entwicklung der Computertechnik eine scharfe Trennung zwischen „statistical“ und „intelligence systems“ immer weniger möglich werde und dass selbst harmlose „statistical systems“ gleichzeitig als „foot in the door“ für weitergehende Systeme wirken

[68] Brenton (1964, S. 13), Hervorhebung im Original.
[69] Brenton (1964, S. 232 f.).
[70] Für eine ausführliche Übersicht, siehe Kamlah (1969, S. 16 f.).
[71] Gallagher nennt das „National Data Center“ darum auch „Dossier Bank“, siehe Gallagher (1967, S. 111).
[72] Zum Hintergrund dieses Reports und dazu, wie er gelesen werden solle und wie nicht, siehe Dunn (1967).

könnten.[73] Unter vielen stark Computer-fixierten Forderungen zum Schutz der *privacy*, die auch von anderen zeitgenössischen Autorinnen und Autoren vertreten wurden, sticht seine Forderung nach der Einführung eines jährlichen Datenbriefes heraus.[74] Das „National Data Center“ wurde dabei vor allem deshalb zentraler Anknüpfungspunkt der politischen *privacy*-Debatte, weil die Verantwortlichen sich schlicht weigerten, angemessen auf die Fragen und Bedenken einer bereits kritischen Öffentlichkeit einzugehen.[75]

Die ersten Ansätze für Anforderungen an technische Systeme selbst wurden 1965 von Paul Baran formuliert. Ausgehend von der Annahme, dass viele *privacy*-Probleme erst durch moderne technische Entwicklungen entstanden seien, müssten diese auch „effective safeguards“ zur Verfügung stellen.[76] Baran formuliert einige grundlegende Prinzipien, von denen einige auch heute noch Gültigkeit verlangen können: eine fundierte und realistische Risikoabschätzung, ein Bewusstsein für ständig komplexer werdende Systeme, die Einbeziehung von „safeguards“ schon in das Systemdesign, ein gesetzliches Verbot „schwacher“ Systeme und die Akzeptanz der damit einhergehenden Kosten. Letztere sieht Baran aber als notwendig an – „a price to society for the privilege of building a potentially dangerous system.“[77] Baran behauptet auch, dass Entwicklerinnen besser nicht auf die Hilfe von Juristinnen hoffen sollten, sondern schlicht auf „gutes Design“ achten müssten. Gesetze allein seien ineffektiv. Daneben schlägt er konkrete „safeguards“ vor: Kommunikations- und Datenverschlüsselung, externes Auditing, Monitoring „abnormaler“ Informationszugriffe, Zugriffsprotokollierung sowie internes Auditing. Er weist auch darauf hin, dass für die Zukunft damit zu rechnen sei, dass bisher unverbundene Systeme zusammengeschlossen werden. Darauf müsse sich frühzeitig vorbereitet werden, um dann sinnvolle Regelungen aufstellen und umsetzen zu können.

Mit der Zunahme populärwissenschaftlicher, aber auch populistischer Abhandlungen über *privacy* und einer steigenden öffentlichen Aufmerksamkeit, die sich auch in zunehmenden gerichtlichen Verfahren niederschlug, sei immer deutlicher geworden, dass *privacy* in erster Linie ein außerrechtliches Konzept geblieben sei, das der Rechtswissenschaft erst tiefgehend erschlossen werden müsse – eine Aufgabe, der sich die Zeitschrift „Law and Contemporary Problems“ mit einer Sonderausgabe stelle.[78] Ein grundlegender Kritikpunkt bezieht sich auf den Begriff *privacy* selbst: Er sei negativ besetzt und impliziere einen Rückzug aus der Gesellschaft, während es doch auch und gerade darum gehe, das Agieren in der Öffentlichkeit selbst zu schützen.[79] Edward Shils hingegen beschreibt *privacy* als „zero-relationship“, als Abwesenheit von Interaktion, Kommunikation und Wahrnehmung in einer sozialen Umgebung, in der diese aber grundsätzlich möglich sind. *Privacy* sei damit Isolation aus freien Stücken.[80] Shils ist auch einer der ersten, die *privacy* mit dem Informationsfluss in Verbindung bringen: „Privacy in one of its aspects may therefore be defined as the existence of a boundary through which information does not flow from the persons who possess it to others.“[81] Die Information müsse sich dabei allerdings auf ein Ereignis aus der Privatsphäre beziehen, nur dann könne das Individuum oder die Gruppe darüber Kontrolle ausüben.[82] *Privacy* sei dann der „social space“ um ein Individuum herum, der

[73] Siehe Miller (1967).
[74] Siehe Miller (1967, S. 55).
[75] Siehe Harvard Law Review (1968) oder auch Miller (1969, S. 1131 ff.).
[76] Baran (1965).
[77] Baran (1965, S. 48).
[78] Havighurst (1966).
[79] Konvitz (1966, S. 279).
[80] Shils (1966, S. 281 f.).
[81] Shils (1966, S. 282).
[82] Shils (1966, S. 283).

dem Individuum wegen dessen Individualität gehöre.[83] Auf diese Kontrollierbarkeit stellt auch Kenneth Karst ab, wenn er von „selective disclosure“ spricht.[84] Während er Probleme wie die tendenziell fehlende Zweckbindung zwar durchaus anspricht, expliziert er nur zwei Forderungen: Zugangsbeschränkungen zu personenbezogenen Daten und Garantie ihrer Vollständigkeit und Korrektheit. Karst formuliert auch eine der ersten Kritiken am Ersatz einer fundierten Erforderlichkeitsprüfung als Voraussetzung einer Veröffentlichung durch die Fiktion der Einwilligung.[85]

Zu den wichtigsten Theoretikern der ersten Stunde der modernen *privacy*-Debatte gehört zweifellos Alan Westin, der 1966 mit zwei Artikeln und einem darauf aufbauenden Buch, das 1967 erschien,[86] und dessen *privacy*-Konzeption bis heute prägend ist. Insbesondere seine allgemeine, in „Privacy and Freedom“ ausgeführte, *privacy*-Definition wird ausgiebig zitiert:

> „Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.“[87]

Westin unterscheidet drei Kategorien von Eingriffen in die *privacy*:

> [...] *physical surveillance*, the observation without his knowledge or consent of a person's location, acts, speech, or private records through listening or watching devices; *data surveillance*, the collection, storage, exchange, and integration of comprehensive documentary information about individuals and groups through computers and other data-processing systems; and *psychological surveillance*, the use of mental testing, drugs, emotion-measuring devices, and other processes to extract information which the individual does not know he is revealing, reveals unwillingly, or discloses without full awareness of the exposure of his private personality.[88]

Alle drei Eingriffskategorien – *physical surveillance*, *data surveillance* und *psychological surveillance* – sind grundsätzlich auch heute noch relevant, wenn auch jeweils nicht in der gleichen Form wie in der Zeit Westins. Für die Ausweitung der *data surveillance*, die hier im Vordergrund stehen soll, macht Westin vier zentrale Entwicklungen verantwortlich: erstens die dramatische Ausweitung des Sammelns und Speicherns von Informationen auch unabhängig von der Computerentwicklung, zweitens die Durchsetzung des Computers, die es öffentlichen und nicht-öffentlichen Organisationen ermöglicht habe, die gespeicherten Informationen effektiver und schneller zu nutzen, drittens die Ausweitung des Informationsaustausches zwischen diesen Organisationen und viertens die absehbare Ersetzung des Bargelds durch elektronisches Geld mit Online-Banking und E-Business.[89] Absehbar sei deshalb das Entstehen vollständiger und zentralisierter elektronischer Identitäten – eines „master computer dossier“[90] – auf der Basis von Personenkennziffern. Westin untersucht die Funktionen, die *privacy* in einer demokratischen Gesellschaft hat. Auf der Ebene des politischen Systems dient *privacy* dabei als Abwehr gegen totalitäre Tendenzen des Staates:[91]

[83] Shils (1966, S. 306).
[84] Karst (1966, S. 344).
[85] Karst (1966, S. 345).
[86] Westin (1966a), Westin (1966b), Westin (1967).
[87] Westin (1967, S. 7).
[88] Westin (1966a, S. 1004), Hervorhebung im Original.
[89] Westin (1966a, S. 1010 ff.).
[90] Westin (1966a, S. 1013).
[91] Westin (1966a, S. 1018 ff.).

> „a balance that insures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relies on publicity as a control of government and privacy as a shield for group and individual life.“[92]

In Interaktionssystemen gebe es vier Arten von *privacy*-Zuständen: *solitude*, *intimacy*, *anonymity* und *reserve*,[93] die zusammen vier Funktionen erfüllen: *personal autonomy*, *emotional release*, *self-evaluation* und *limited and protected communication*.[94] Westins Autonomie- und Individualitätskonzeption basiert dabei auf einem Sphärenmodell, dass er aus der Mikrosoziologie – so zitiert er etwa Georg Simmel, Robert Ezra Park und Erving Goffman – übernimmt.[95] Westin schlussfolgert: „But privacy is neither a self-sufficient state nor an end in itself, even for the hermit and the recluse. It is basically an instrument for achieving individual goals of self-realization.“[96] Nicht nur Individuen, sondern auch Organisationen hätten ein Interesse an *privacy*, die dort die grundlegend gleichen Funktionen erfüllten.[97] Auch bei der Betrachtung der Funktionen, die der jeweilige *privacy*-Eingriff spielt, trennt Westin konsequent zwischen Interaktions- und Funktionssystemen – auch wenn er sie nicht so bezeichnet – und unterscheidet sich damit stark von den meisten der ihm Folgenden.[98] Zur Abwägung zwischen den beteiligten Interessen *disclosure* und *surveillance* auf der einen und *privacy* auf der anderen Seite schlägt Westin einen fünfschrittigen Prozess vor.[99] In einem ersten Schritt müsse die Ernsthaftigkeit des Überwachungsbedürfnisses gemessen und im zweiten Schritt die Erforderlichkeit der Mittel geprüft werden. Im dritten Schritt müsse festgelegt werden, welche Anforderungen an die Geeignetheit und Zuverlässigkeit der Mittel zu stellen seien. Dann müsse in einem vierten Schritt geprüft werden, ob eine – grundsätzlich vorherige und informierte – zweckgerichtete Einwilligung eingeholt werden könne, wobei insbesondere die Freiwilligkeit sichergestellt werden müsse. Für implizite Einwilligungen müssten besondere Anforderungen gelten. Im fünften und letzten Schritt müssten Bedingungen und Grenzen der Datenverarbeitung geregelt werden. Dazu gehöre die Frage, wer erheben oder speichern dürfe, welche Datenmenge erhoben werden dürfe und wie lange die Daten gespeichert werden dürfen. Außerdem müsse es eine unabhängige Aufsichts- und Prüfbehörde geben, die den Betroffenen Rechtsschutz garantieren könne. Zuletzt seien Regeln für Datenweitergabe und -nutzung festzulegen.

Westin stellt fest, dass die von ihm geforderten technischen Maßnahmen – etwa Zugriffsbeschränkungen, Verschlüsselung oder Protokollierungssysteme in den drei Systemteilen Eingabe, Speicherung, Ausgabe – nur eine Hälfte aller erforderlichen Schutzmaßnahmen darstellen könnten. Die andere Hälfte bestehe aus passenden ethischen und rechtlichen Regelungen.[100] So schlägt er vor, personenbezogene Daten („personal information“) rechtlich als Eigentumsrecht zu werten und damit dem gleichen Schutz zu unterwerfen, den das Eigentum in den USA hat. Damit sollten Haftungsregeln einhergehen: der Zwang zur Einhaltung rechtstaatlicher Prinzipien bei der

[92] Westin (1966a, S. 1019).
[93] Westin (1966a, S. 1020 ff.).
[94] Westin (1966a, S. 1022 ff.).
[95] Westin (1966a, S. 1022 f.).
[96] Westin (1966a, S. 1029).
[97] Westin (1966a, S. 1031 ff.).
[98] Westin (1966a, S. 1040 ff.).
[99] Westin (1966b, S. 1205 ff.).
[100] Westin (1967, S. 324).

Nutzung von Daten, das Recht informiert zu werden, wenn die Daten in zentralen Datenbanken gespeichert würden, Auskunfts- und Widerspruchsrechte.[101]

Nach der Rechtswissenschaft machte 1967 auch die Computer Science das *privacy*-Problem zum Thema einer wissenschaftlichen Konferenz, der *Spring Joint Computer Conference*. Im Gegensatz zu Westins auch heute durchaus noch tauglicher Definition von *privacy* war die von den anwesenden Informatikern präsentierte schon damals schlicht absurd: Während *security* dem Schutz von Militärgeheimnissen diene, diene *privacy* dem Schutz von Privatgeheimnissen.[102] Trotzdem blieb dieses „privacy as confidentiality"-Paradigma in der Informatik jahrzehntelang wirkmächtig.[103] Insbesondere erklärt sich damit der langjährige Forschungsfokus auf Zutritts-, Zugangs- und Zugriffskontrollsystemen, Protokollierungsmechanismen, Übertragungsverschlüsselung und Anonymisierungstechniken – die *security*-Forschung war offenkundig auf der Suche nach einem von ihr und mit ihren Mitteln lösbaren Problem und fand es fälschlicher Weise in der *privacy*.

Es gab allerdings nicht nur solche, für die weitere Entwicklung *privacy*- und datenschutzfreundlicher Technik wenig hilfreichen Wortmeldungen. Baran wies bereits Ende der sechziger Jahre darauf hin, dass es in Zukunft billiger sein würde, Daten zeitlich unbeschränkt aufzubewahren und dafür immer wieder neue Speichermedien zu kaufen, als sie aus Datenverarbeitungsanlagen zu löschen.[104] Unabhängig von einem Verlust zukünftiger Datenverwendungsmöglichkeiten für die Datenverarbeiter ist eine Löschpflicht demnach schon seit dieser Zeit eine der Technik zu oktroyierende Anforderung, die der technischen Entwicklung und der daraus folgenden Preisentwicklung widerspricht. Auch die Folgen, die sich aus der beliebigen Verkettbarkeit existierender personenbezogener Informationen ergeben, die jeweils einzeln – also: unverkettet – aus *privacy*-Sicht unproblematisch sein mögen, werden schon Ende der sechziger Jahre problematisiert.[105]

Der zweite herausragende *privacy*-Theoretiker neben Alan Westin Ende der sechziger Jahre war Arthur Miller, der in seinem für die *privacy*-Debatte zentralen Werk[106] die Folgen des Computers als dem zentralen Medium der Informationsgesellschaft für die *privacy* des Individuums analysiert:

> The assumption throughout is that the computer is not simply a sophisticated indexing machine, a miniaturized library, or an electronic abacus; it is the keystone of a new communications medium that eventually will have global dimensions.[107]

Aus der Sicht des Individuums liege das zentrale Problem im Verlust der Kontrolle über die sie betreffenden Informationen und ihre Verbreitung – „deprivation of access control"[108] – sowie über deren faktische und kontextuelle Korrektheit – „deprivation of accuracy control".[109] Gesellschaftlich bestehe das Problem der Entwicklung hin zu einem Überwachungsstaat:

> As might be expected, the proponents of these pervasively intrusive systems assert that they will be used only for »ethical« and »benevolent« purposes; but the enor-

[101] Westin (1967, S. 324 f.).
[102] Vergl. Ware (1967a); Ware (1967b); Petersen und Turn (1967); Titus (1967).
[103] Siehe Gürses (2010).
[104] Siehe Baran (1968, S. 9).
[105] Siehe Harvard Law Review (1968, S. 410).
[106] Miller (1969).
[107] Miller (1969, S. 1093). Siehe dort auch S. 1100 ff. und S. 1165 für weitere Ausführungen zur zukünftigen Verschmelzung von Datenverarbeitung und Kommunikation in einem gemeinsamen technischen System und dessen Ausbreitung bis in die privaten Haushalte.
[108] Siehe Miller (1969, S. 1109 ff.).
[109] Siehe Miller (1969, S. 1114 ff.).

> mous potential for abuse inherent in surveillance procedures of this type makes one wonder whether the assurances of these advocates are sufficient protection.[110]

Miller weist auch darauf hin, dass sich die Sensitivität von Informationen nicht aus den Informationen selbst ableiten lässt – sie ist also keine intrinsische Eigenschaft –, sondern variiert nach den Umständen von Datenverarbeitung und Datenweitergabe sowie den beteiligten Organisationen.[111] Zur Sicherstellung der *privacy* schlägt Miller neben sicherheitstechnischen Mechanismen[112] wie Zugriffskontrollen, zertifizierter Software und organisatorischen Sicherheitsmaßnahmen auch explizite *privacy*-Maßnahmen vor, da Technik allein *privacy* nicht garantieren könne.[113] Der aus Millers Sicht wichtigste Grundsatz ist jedoch die Datensparsamkeit: „a regulatory scheme that focuses on the end use of the data by governmental or private systems might be a case of too little, too late.“[114] Vorschläge wie die Gewährung von Eigentumsrechten oder eigentumsähnlichen Rechten an die Betroffenen, wie etwa von Westin vertreten, lehnt Miller wegen fehlender Vereinbarkeit mit den durch *privacy* zu schützenden Werten ab.[115] Stattdessen schlägt er ein Verbot mit Erlaubnisvorbehalt vor, wie es heute auch im deutschen und europäischen Datenschutzrecht gilt.[116]

Zwei Jahre nach seinem auf die wissenschaftliche Debatte zielenden Beitrag publiziert er mit dem Buch „The Assault on Privacy“[117] ein eher populärwissenschaftliches Werk, dessen Verdienst vor allem darin besteht, die politischen Hintergründe zu beleuchten. So beschreibt er ausführlich, wie Menschen und Gruppen in den USA von verschiedenen staatlichen Organisationen überwacht werden. Betroffen sind dabei vor allem politische Gruppen, die sich kritisch zum Vietnamkrieg, zur Rassentrennung oder zum Umgang mit politischen Freiheitsrechten äußern.[118] Miller beschreibt den Widerstand gegen das Nationale Datenzentrum als gegen eine in *privacy*-Fragen völlig ignorante – und somit angreifbare – Gruppe von Fürsprecherinnen. Die Ignoranz in Datenschutzfragen, das Bestehen auf einer Unterscheidung zwischen *statistical* und *intelligence data* auch gegen kritische Nachfragen und – ganz allgemein – die Nichtreaktion auf die Befürchtungen von Interessierten: Dies alles war wie ein Tropfen, der ein Fass zum Überlaufen brachte. Den Sieg über das Nationale Datenzentrum bezeichnet Miller als Pyrrhussieg: Mit dem Wegfall des Datenzentrums falle auch die Möglichkeit einer föderalen Regulierung der *privacy* weg.[119] Langfristig hat Miller für die USA damit Recht behalten.

[110] Miller (1969, S. 1123). Zur aus der Überwachung folgenden Machtimbalance zwischen Individuum und staatlicher oder privater Organisation siehe dort auch S. 1176.

[111] Siehe Miller (1969, S. 1188).

[112] Siehe Miller (1969, S. 1207 ff.). Wo er über technische Maßnahmen schreibt, bezeichnet er sie durchgängig als „security methods“. Trotzdem bleibt unklar, ob er damit tatsächlich ausdrücken will, dass *privacy* und *security* zwei unterschiedliche Konzepte seien und *security* nur notwendige, nicht aber hinreichende Bedingung für die Sicherstellung von *privacy* sein könne.

[113] Siehe Miller (1969, S. 1214). Unter anderem schlägt er eine Maßnahme vor, die heute als k-Anonymität bezeichnet wird, allerdings nicht nur bei der Aus- oder Weitergabe von Informationen, sondern schon bei deren Eingabe, siehe S. 1216 f.

[114] Miller (1969, S. 1221). Diese Trennung zwischen dem Problem, das geregelt werden soll, und dem Regelungsansatz ist offenbar weitgehend unverstanden geblieben, siehe etwa Cate (2006). Zwar ist es in erster Linie die Nutzung der Informationen, die problematisch ist, sie kann aber eben – jedenfalls nach Meinung der meisten Datenschutzvertreterinnen der 1960er und 1970er – nicht sinnvoll zum Regelungsansatz gemacht werden. Eine Kritik an dieser Trennung muss an ihrer Begründung ansetzen, nicht nur oberflächlich am Fakt der Trennung.

[115] Siehe Miller (1969, S. 1223 ff.).

[116] Siehe Miller (1969, S. 1234 f.).

[117] Miller (1971).

[118] Siehe Miller (1971, S. 39 ff.).

[119] Miller (1971, S. 57 ff.).

Neben staatlichen Datensammlungen betrachtet Miller die privatwirtschaftliche Erhebung und Nutzung von personenbezogenen Daten als zweiten großen Problembereich für die *privacy* und dabei insbesondere das Kredit- und Kreditauskunftsgeschäft.[120] Der 1969 beschlossene Fair Credit Reporting Act wird von Miller ausführlich kritisiert. Das Gesetz würde kein einziges seiner erklärten Ziele erreichen, es sei eher ein Schutzgesetz für Kreditauskunfteien gegen von Datenmissbrauch Betroffene.[121]

Miller verweist darauf, dass Computersysteme speichern könnten, aus welchen Quellen Daten ursprünglich stammten, d. h. welche Stelle die Daten weitergegeben hat. Damit könne auch weitergegeben werden, welchen spezifischen rechtlichen Regelungen diese Daten unterliegen.[122]

Miller stellt verschiedene Möglichkeiten vor, wie das amerikanische Recht das Problem der *privacy* angehen könnte. Zuerst wendet er sich der Theorie zu, die vorschlägt, das *right of privacy* als Eigentumsrecht zu fassen. Der Ansatz werde von Westin und Shils vertreten, sei aber schon von Warren und Brandeis als unsinnig abgelehnt worden. Es gehe grundsätzlich nicht um ökonomische, sondern um urpersönliche Interessen, sowie individuelle, menschliche Werte und emotionale Zustände. Die Verantwortung für den Schutz der Interessen würde einseitig auf die Betroffene verlagert, anstatt dass klare Pflichten oder Beschränkungen für die datenverarbeitenden Stellen aufgestellt würden.[123] Eine zweite Meinung will personenbezogene Daten an Informationstreuhänder übertragen, die die Daten gemäß einem Treuhandvertrag verwalten und eine vertragskonforme Nutzung garantieren. Miller weist darauf hin, dass dieses Modell keinen allgemeinen Missbrauchsschutz biete, sondern beschränkt sei auf diejenigen Stellen, die sich für die Nutzung der Daten den Regeln des Treuhänders unterwerfen. Auch werde dabei die Datenerhebung völlig unreguliert gelassen.[124] Gleiches gelte für gewährleistungsrechtliche Ansätze. Miller verweist hier darauf, dass mit der Gewährleistung etwa die Korrektheit der Daten zugesichert werden solle, und kritisiert diese Herangehensweise, weil das schon durch das *law of defamation* getan werde. Auch die Anlehnung der *privacy* an das Recht der Vertraulichkeit und Geheimhaltungsverpflichtungen lehnt er ab.[125]

Miller wendet sich aus praktischen Erwägungen gegen eine komplexe und gleichzeitig kleinteilige – und technikzentrierte – Regulierung und plädiert stattdessen für einen weniger ambitionierten Ansatz eines „general standard of care to be followed by data handlers“.[126] Eine solche gesetzliche Regelung müsse sowohl öffentliche als auch private Datenverarbeitung umfassen.

Auch M. G. Stone und Malcolm Warner betrachten *privacy* ausschließlich im Verhältnis zwischen Individuum und Organisation, für das sie eine Machtimbalance statuieren, die durch den Einsatz von Computern zunehmen werde: „More information, more rational judgments. Better data, better decisions. More facts, more power.“[127] Es gehe dabei nicht um eine Kontrolle des Menschen durch den Computer, sondern um den Machtzuwachs der Organisation, die die Computer einsetze. „The computer has given bureaucracy the gift of omniscience, if not omni-

[120] Miller (1971, S. 68 ff.).
[121] Miller (1971, S. 86 f.). Siehe aber auch die Einschätzung von Hoofnagle (2013), dass der Fair Credit Reporting Act einen besseren Schutz vor Big Data biete als alle aktuellen Vorschläge. Das muss jedoch kein Widerspruch sein, sondern kann auch nur darauf hindeuten, wie schlecht die derzeit diskutierten Vorschläge sind.
[122] Miller (1971, S. 144). Diese technische Bindung von rechtlichen Anforderungen direkt an die einzelnen Datensätze werden seit den 1990er Jahren als „sticky policies“ bezeichnet. Trotz klarer Hinweise auf *prior art* konnten sie von HP patentiert werden.
[123] Miller (1971, S. 211 ff.).
[124] Miller (1971, S. 216 ff.).
[125] Miller (1971, S. 219 f.).
[126] Miller (1971, S. 224 f.).
[127] Stone und Warner (1969, S. 258).

potence, by putting into its hands the power to *know*. No fact unrecorded, nothing forgotten nor lost, nothing forgiven."[128] Es gelte zu verhindern, dass eine „infra-structure of tyranny" entstehe. Dazu müsse insbesondere auch sichergestellt werden, dass die Informationen nicht verkettet werden:

> It is important that information relating to criteria by which the claims of citizens could be judged is *kept* un-integrated. Honesty should be presumend, as it is now, in each sphere of the person's relations with the State, unless there is *specific* evidence to the contrary—just as in law innocence is the primary presumption in all cases. When records are integrated, the picture could be changed.[129]

Wie Westin und Miller erweiterten auch Stone und Warner ihre Ausarbeitung zu einem Buch, das sie 1970 unter dem Titel „The Data Bank Society" publizierten.[130] Darin bezeichneten sie das Verhalten von Organisationen bzgl. der Informationsverarbeitung als Spezialfall des Parkinsonschen Gesetzes: Je größer die Fähigkeit von Organisationen zur Verarbeitung von Informationen sei, desto mehr Informationen verlange sie.[131] Gespeicherte Fakten würden zur Wahrheit, weil sie gespeichert seien. Und als solche würden sie dann zur Grundlage von Entscheidungen.[132] Sie zitieren Stafford Beer:

> „My electronic image in the machine may be more real than I am. It is rounded; it is complete; it is retrievable; it is predictable in statistical terms. ... There is no ambiguity, no loss of history, no rationalization. I am a mess; and I don't know what to do. The machine knows better – in statistical terms. Thus is my reality less real than my mirror image in the store. That fact diminishes me." [133]

Es müsse sichergestellt werden, dass „separate files are *not* integrated, and *not* cross-referenced, so that *data collected for one purpose is never used for any other*."[134] Außerdem müsse die Gewaltenteilung zwischen lokalen und nationalen Stellen aufrechterhalten werden.[135] Warner und Stone führen auch eine frühe Auseinandersetzung mit Positionen, wie sie heute von der sogenannten *post-privacy*-Bewegung vertreten werden: Anthony Wedgwood Benn, ein Labour-Politiker,

> „points out that only in a world of total information could we take off the fig-leaf which Adam and Eve were compelled to don when they ate of the tree of knowledge, and forgot the fact that people need not hide things about themselves. Against this view, we feel that the citizen *should* have the option of concealing or revealing personal affairs, whether to others, or the State; and would consider a world of *total* information probably impossible to achieve anyway or, if possible to achieve, a nightmare."[136]

Nicht zuletzt sind sie auch nicht verlegen um große Worte:

[128] Stone und Warner (1969, S. 260).
[129] Stone und Warner (1969, S. 263 f.). Der Begriff der Verkettung ist dabei das moderne Äquivalent des damals gebräuchlichen Begriffs der Integration.
[130] Warner und Stone (1970).
[131] Warner und Stone (1970, S. 23).
[132] Warner und Stone (1970, S. 67).
[133] Stafford Beer, Computer Weekly, 21. August 1969, zitiert nach Warner und Stone (1970, S. 156).
[134] Warner und Stone (1970, S. 179).
[135] Warner und Stone (1970, S. 179).
[136] Warner und Stone (1970, S. 223).

> „»Man was born free, but everywhere he is on tape! Workers of the world unite; you have nothing to lose but your IBM card!« – there is the political slogan for the future.“[137]

Nicht nur, dass die Macht von Organisationen auf Kosten der Individuen zunehmen würde, den Informationssystemen wohne auch eine Tendenz zur Zentralisierung inne, so Jeffrey A. Meldman.[138] Das gelte sowohl für *intelligence systems* wie für *statistical systems*, obwohl sie in der öffentlichen Debatte als grundsätzlich verschiedene Systeme wahrgenommen würden, wobei der Unterschied zwischen beiden nur in der Ausgabe liege: beide Systeme speicherten die Daten personenbezogen, aber *statistical systems* würden nur anonymisierte Daten ausgeben.[139] Meldman hält das nicht für ausreichend und verlangt den Einsatz von Pseudonymisierungstechniken.[140]

Die immer lauter erhobenen Forderungen nach gesetzgeberischen Maßnahmen riefen auch Kritikerinnen auf den Plan, die stattdessen vorschlugen, dass die Industrie Maßnahmen des Gesetzgebers zuvorkommen müsse. Aus kartellrechtlichen Gründen und zur besseren Durchsetzung wurde die Form der regulierten Selbstregulierung vorgeschlagen.[141] Die beiden zentralen Ziele der Selbstregulierung, „that computer systems which handle sensitive individual or proprietary data will meet certain minimum standards established for the protection of privacy“ und „that computer system operators will be able to continue to operate in a competitive economy unhindered by either overly restrictive governmental regulation or the fear of private legal liability“,[142] prägen die Selbstregulierungsdiskussion bis heute. Andererseits war vorgesehen, dass Systeme, die nicht nachweisen können, dass sie die Anforderungen der „industry standards for the protection of privacy and security of data“ erfüllen, nicht betrieben werden dürfen.[143]

Bis zum Ende der sechziger Jahre waren bereits mehr als 600 Arbeiten zum Themenbereich Computer und *privacy* erschienen.[144] Die meisten davon drehten sich immer um die gleichen Topoi: IT-Sicherheitsmaßnahmen wie *access control*, Verschlüsselung und Protokollierung sowie die Korrektheit und Vollständigkeit von Informationen.[145] Daneben tauchten aber auch die ersten Vorschläge zur technischen Umsetzung von originären *Privacy*-Anforderungen auf: Edgar L. Feige und Harold W. Watts lieferten etwa einen ersten Vorschlag für die Anonymisierung von personenbezogenen Informationen in Datenbanksystemen durch Datenaggregation.[146] Alexander W. Astin und Robert F. Boruch schlagen ein manuelles Verfahren zur Sicherstellung der Anonymität in statistischen Datenbanken vor: Zum Schutz sowohl vor staatlichen Herausgabeansprüchen als auch vor unzulässiger Einsichtnahme und Weitergabe durch die Betreiber sollen die Informationen von Beginn an nur pseudonymisiert gespeichert werden, während die Zuordnungsliste außerhalb der eigenen Jurisdiktion aufbewahrt werde.[147] Dieser „linking service“ solle, so Astin und Boruch, weltweit in einem auf Gegenseitigkeit basierenden System aufgebaut werden.

[137] Warner und Stone (1970, S. 80 f.).
[138] Meldman (1969).
[139] Meldman (1969, S. 338).
[140] Meldman (1969, S. 354).
[141] Siehe etwa Grenier (1970).
[142] Grenier (1970, S. 496).
[143] Grenier (1970, S. 508).
[144] Siehe Harrison (1967) und Harrison (1969).
[145] Siehe beispielhaft Garrison und Ramamoorthy (1970) oder Hellman (1970).
[146] Feige und Watts (1970). Die Autoren weisen allerdings auch darauf hin, dass diese Anonymisierung durch Zusatzwissen ausgehebelt werden könne, siehe Feige und Watts (1970, S. 267).
[147] Astin und Boruch (1973).

Während etwa Miller darauf hinwies, dass die Sensitivität von Informationen keine intrinsische Eigenschaft sei, versucht Jon Bing in einer ausführlichen Studie, genau dieses zu belegen und ein passendes Klassifikationsschema zu entwerfen.[148] Tatsächlich bewertet er aber nicht die Sensitivität der Informationen selbst, sondern die Sensitivität ihrer Verarbeitung, weil er versucht, alle Umstände der Informationsverarbeitung in seine „Berechnung" der Maßzahl einzubeziehen.[149] Am Ende ist seine Liste der einzubeziehenden Faktoren so groß, dass sie keinen Vorteil gegenüber einer „normalen" Risikoabschätzung der Informationsverarbeitung insgesamt bietet. Vor allem aber wird damit deutlich, dass alle verkürzenden Sensitivitätsangaben untauglich sind.[150]

Lance J. Hoffman und William F. Miller führen 1973 den ersten bekannten erfolgreichen Angriff auf anonymisierte Informationen in statistischen Datenbanken aus und können diese unter Verwendung von Zusatzwissen deanonymisieren.[151] Damit zeigen sie, dass Feige und Watts zu Recht gewarnt hatten, und fordern, dass statistische Datenbanken erstens keine Ergebnisse für sehr kleine Gruppen ausgeben dürften und zweitens eine eingebaute Angriffserkennung besitzen müssten.[152]

Parallel wurden weitere Arbeiten veröffentlicht, die versuchten, das *privacy*-Problem genauer zu beschreiben und – vor allem rechtliche – Lösungen anzubieten.

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) gründete 1968 eine Arbeitsgruppe zur Computernutzung in den OECD-Ländern, die 1970 die Auswirkungen der elektronischen Datenverarbeitung auf die *privacy* untersuchte. Der Untersuchungsbericht wurde von G. F. B. Niblett erstellt und 1971 veröffentlicht.[153] Niblett hält *privacy* für das Bedürfnis von Individuen, den Fluss von Informationen über sich selbst zu kontrollieren.[154] Auf der Basis von drei für das *privacy*-Problem konstitutiven Phasen der Informationsverarbeitung – Erhebung/Sammlung (*collection*), Auswertung/Nutzung (*analysis and evaluation*) und Übermittlung/Weitergabe (*transmission*) von Daten – versucht er dann, Gefahren zu identifizieren und schlägt mögliche Gegenmaßnahmen vor, wobei er keine neuen Erkenntnisse vermittelt.

Klaus Lenk stellt fest, dass es drei Gruppen gebe, die sich mit öffentlichen Datenbanken beschäftigten – 1. Computerspezialistinnen, 2. Bürgerrechtlerinnen und Datenschützerinnen sowie 3. Politikerinnen und Menschen aus der Verwaltung – und die, trotz teilweise jahrelanger, scharf geführter Diskussion – immer noch keine gemeinsame Sprache sprechen würden. Dies führe zu Unklarheiten und verhindere Lösungen.

> „The negative consequences of computerised data banks that contain data which can be related to persons, are commonly described as threats to personal privacy. Yet the concept of privacy is not a very clear one. It largely depends on the different social and legal systems of the countries concerned. To define privacy with regard to government action is equivalent to determining how much and what kind of control of the citizens should be conceded to the government. To a large extend, this means

[148] Bing (1972). Laut Steinmüller (1993, S. 669, Fn. 599 (auf S. 835)) habe Bing den Beitrag „später zurückgezogen".

[149] Siehe Bing (1972, S. 101 ff.). Dazu gehören etwa die Anzahl der Betroffenen, die möglichen Empfängerinnen mit ihrer Funktion, ihrer Größe sowie ihren ethischen Standards, der Zweck der Informationsverarbeitung, der Kontext, die gesellschaftliche Wahrnehmung der betreffenden Informationen und „andere Gesichtspunkte".

[150] Bis heute hält das Gesetzgeber nicht davon ab, die „Sensitivität von personenbezogenen Daten" zum Maßstab gesetzlicher Anforderungen zu machen. Es sieht ja auch alles so einfach aus, wenn frau ein – möglicherweise noch zweiwertiges – Klassifikationsschema in die Luft malt…

[151] Hoffman und Miller (1973).

[152] Siehe auch den etwa zeitgleich erschienenen Beitrag von Jacobs (1973) über die Unwirksamkeit der Deanonymisierung der Studentinnenstatistik.

[153] Niblett (1971).

[154] Niblett (1971, S. 18).

> that availability of person-related information considerably facilitates the exercise of power on individuals and thus increases this power. This concerns private power as well as the State [...].“[155]

Die umfassendste Auseinandersetzung Anfang der 1970er Jahre mit der Frage, was *privacy* eigentlich sei, wurde in einem Tagungsband der *American Society for Political and Legal Philosophy* niedergelegt.[156] Stanley I. Benn verweist auf drei persönliche Ideale, die im Zentrum der liberalen individualistischen Tradition stünden: „The first is the ideal of personal relations; the second, the Lockian ideal of the politically free man in a minimally regulated society; the third, the Kantian ideal of the morally autonomous man, acting on principles that he accepts as rational.“[157] Dabei sei gerade das zweite Ideal zentral für die *privacy* und beschreibe ein Leben, in dem „first, the average individual is subject only within reasonable and legally safeguarded limits of the power of others, and, second, where the requirements of his social roles still leave him considerable breadth of choice in the way he lives.“[158] Machtbeschränkung und rollenspezifische Freiheiten stünden demnach im Zentrum. Hingegen sieht W. L. Weinstein in der *privacy* schlicht ein Gegenstück zur Öffentlichkeit.[159] Elizabeth L. Beardsley kritisiert Westins *privacy*-Konzept als zu kurz gegriffen. Stattdessen müssten zwei Aspekte fundamental unterschieden werden: Autonomie im Sinne einer allgemeinen Handlungsfreiheit auf der einen sowie das Recht auf „selective disclosure“ auf der anderen Seite.[160] M. A. Weinstein betrachtet *privacy* als einen Zustand des „being-apart-from-others“, d. h. als eine private oder geheime Sphäre. „It is voluntary limitation of communication to or from others for the purpose of undertaking activity in pursuit of a perceived good.“[161] Carl J. Friedrich erklärt *privacy* schlicht zu einem Aspekt von *secrecy*, zur „functional secrecy“.[162] Ernest van den Haag hält *privacy* für einen „extended part of the person“ und behauptet, dass es am besten als Eigentumsrecht behandelt werden sollte. *Privacy* ist dann „the exclusive right to dispose of access to one's proper (private) domain.“[163] Für Hyman Gross ist *privacy* notwendig „to maintain an integrated personality in a social setting“. Individuen seien daher immer darauf bedacht zu kontrollieren, wie sie auf andere wirken. Das tiefere Motiv sei dabei „to influence the reactions of others, and this is at the heart of human social accommodation.“[164] *Privacy* habe dabei nichts mit Scham zu tun, sondern Scham entstünde auf Seiten des Betroffenen gerade dadurch, dass ihr die Kontrolle darüber entzogen werde, „who else shall know it and what use shall be made of it.“[165] Paul A. Freund vergleicht das *right to privacy* mit dem allgemeinen Persönlichkeitsrecht und kommt zu dem Ergebnis, dass beide äquivalent seien, obwohl ersteres seit Prosser als ein mehrere unterschiedliche Rechtsgüter umfassendes Konzept verstanden werde, das allgemeine Persönlichkeitsrecht jedoch als ein holistisches Prinzip.[166]

Im Auftrag der *Russell Sage Foundation* und des *Computer Science and Engineering Board* der *National Academy of Sciences* führten Alan F. Westin und Michael A. Baker zwischen 1970 und

[155] Lenk (1972, S. 5 f.).
[156] Pennock und Chapman (1971).
[157] Benn (1971, S. 15 f.).
[158] Benn (1971, S. 21).
[159] Weinstein (1971b).
[160] Beardsley (1971).
[161] Weinstein (1971a, S. 104).
[162] Friedrich (1971).
[163] van den Haag (1971, S. 151).
[164] Gross (1971, S. 173).
[165] Gross (1971, S. 177).
[166] Freund (1971).

1972 eine großangelegte Untersuchung über die Datenverarbeitung in 55 großen öffentlichen und privaten Organisationen durch: „The Project on Computer Databanks“, deren Ergebnisse 1972 als „Databanks in a Free Society: Computers, Record-Keeping and Privacy“ veröffentlicht wurden.[167] Bei der Untersuchung handelte es sich im wesentlichen um eine Weißwäsche staatlicher und privater Datenverarbeitungs- und Überwachungssysteme. Behauptungen der Organisationen über ihren Umgang mit personenbezogenen Daten wurden nicht hinterfragt, sondern als Tatsachen behandelt.[168] Auf diese Weise war die Untersuchung nicht einmal theoretisch geeignet, Datenschutzverletzungen zu entdecken. Auch wurde etwa der Verkauf personenbezogener Daten aus staatlichen Informationssystemen schlicht deshalb nicht als *privacy*-Verletzung betrachtet, weil er gesetzlich geregelt sei und weil die Daten als „öffentlich“ deklariert wurden.[169] Die Autoren wollen aus ihren Untersuchungen drei Schlussfolgerungen gezogen sehen:

> „First, computer usage has not created the revolutionary new powers of data surveillance predicted by some commentators. [...] Second, computerizations is definitely bringing some important increases in the efficiency of organizational record-keeping. [...] However, even where these increases in efficiency are taking place, organizational policies which affect individual rights are still generally following the precomputer patterns in each field of record-keeping.“[170]

Im Gegensatz dazu untersuchte das *Advisory Committee on Automated Personal Data Systems* des *U.S. Department of Health, Education & Welfare* unter Leitung von Willis H. Ware die gesellschaftlichen Auswirkungen des Einsatzes von Computern bei der Verarbeitung personenbezogener Informationen nicht nur auf der Basis von Eigenaussagen der Datenverarbeiterinnen und kam damit zu gegenteiligen Ergebnissen.[171] Zentraler Untersuchungsgegenstand ist dabei das Verhältnis zwischen Individuen und informationsverarbeitenden Organisationen und die Herausforderungen, die die Datenverarbeitung für die überkommenen rechtlichen und sozialen Kontrollmöglichkeiten gegenüber diesen Organisationen erzeugen würden.[172] Der Report stellt fest,

> „that the net effect of computerization is that it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems. Even in non-governmental settings, an individual's control over the use that is made of personal data he gives to an organization, or that an organization obtains about him, is lessening.“[173]

Aus diesem Grund schlägt der Report die Einführung eines föderalen „Code of Fair Information Practice“ für alle automatisierten Informationssysteme vor, die personenbezogene Daten verarbeiten. Dieser Code basiert auf fünf grundlegenden Prinzipien: 1. keine geheimen Systeme, 2. Auskunftsrecht der Betroffenen, 3. Zweckbindung, 4. Berichtigungsrecht der Betroffenen, 5.

[167] Westin und Baker (1972).
[168] Westin und Baker (1972, S. 4). Siehe auch die Aussage: „First, our focus is deliberately empirical. Rather than discussing hypothetical uses of the computer and its »potential« capabilities—an approach which has led to great confusion in the public's understanding of the computer's impact on record-keeping—we report what we found to be happening today in the 55 computerizing organizations we studied.“ Westin und Baker (1972, S. 217). Weil keine Verstöße bekannt seien, habe es keine gegeben!
[169] Westin und Baker (1972, S. 72 ff.).
[170] Westin und Baker (1972, S. 341).
[171] U.S. Department of Health, Education, and Welfare (1973).
[172] U.S. Department of Health, Education, and Welfare (1973, S. 9 f.).
[173] U.S. Department of Health, Education, and Welfare (1973, S. xx).

Pflicht für Organisationen zu organisatorischen und technischen Schutzmaßnahmen.[174] Dieser verfahrensorientierte Ansatz wurde unter anderem deshalb gewählt, weil er als eine notwendige Folge der Abbildung eines allgemeinen *right to privacy* auf die Informationsverarbeitung durch Organisationen gesehen wurde: Durch den grundsätzlich von beiden Seiten geteilten Verarbeitungszweck müsse „[p]ersonal privacy, as it relates to personal-data record keeping [...] be understood in terms of a concept of mutuality."[175] Daneben werden beispielhaft Fragen angegeben, die bei der Gestaltung eines „personal data system" zu beantworten seien, wie etwa: „How might the same purpose be accomplished without collecting these data?"[176] Der hier niedergelegte Code bildet die Grundlage des US Privacy Act of 1974.[177]

James B. Rule analysiert das *privacy*-Problem als Ausprägung und Folge einer zunehmenden Bürokratisierung: „of large organizations, precise rules and formal criteria for action."[178] Anhand der Analyse von fünf modernen Großorganisationen und deren Informationsverarbeitungspraktiken[179] – „systems of mass surveillance and control"[180] – untersucht er die „changing mechanisms and patterns of social control associated with the growth of increasingly modern social structures"[181] auf der Basis der soziologischen Theorie Talcott Parsons. Solche Systeme seien charakteristische Produkte der modernen Gesellschaften, die sie hervorgebracht haben. Sie würden vor allem entstehen, wenn fünf Bedingungen erfüllt seien:

> „1. When an agency must regularly deal with a clientele too large and anonymous to be kept track of on a basis of face-to-face acquaintance;
> 2. When these dealings entail the enforcement of rules advantageous to the agency and potentially burdensome to the clientele;
> 3. When these enforcement activities involve decision-making about how to act towards the clientele [...];
> 4. When the decisions must be made discriminatingly, according to precise details of each person's past history or present situation;
> 5. When the agency must associate every client with what it considers the full details of his past history, especially so as to forestall people's evading the consequences of their past behaviour."[182]

Die entstehenden Informationssysteme erweiterten die Fähigkeiten der Organisationen, ihre Ziele auch auf Kosten der Betroffenen zu erreichen.[183] Sie seien daher als Systeme der Macht im Sinne Max Webers zu bezeichnen. Die (Wieder-)Herstellung von Gerechtigkeit im Sinne eines gerechten Interessenausgleichs zwischen der bürokratischen Organisation auf der einen sowie dem Individuum und der Gesellschaft auf der anderen Seite erfordere dabei „control and hence standardization of data processes."[184]

[174] U.S. Department of Health, Education, and Welfare (1973, S. 41).
[175] U.S. Department of Health, Education, and Welfare (1973, S. 40).
[176] U.S. Department of Health, Education, and Welfare (1973, S. 51).
[177] Siehe umfassend und auch zur Kritik an den Lücken, die das Gesetz lässt, Regan (1988).
[178] Rule (1973, S. 14).
[179] Dazu gehören die polizeiliche Datenverarbeitung in Großbritannien, das britische Kfz- und Führerscheinverwaltungssystem, das britische Versicherungssystem, das US-amerikanische System der Konsumentinnenkreditüberwachung sowie das BankAmericard-System.
[180] Rule (1973, S. 29).
[181] Rule (1973, S. 15).
[182] Rule (1973, S. 29).
[183] Rule (1973, S. 274 f.).
[184] Rule (1973, S. 285).

Irwin Altman, dessen sozialpsychologische Theorien auch heute noch und vor allem sachlich falsch angewandt werden, definiert *privacy* als Prozess der „interpersonal boundary regulation“, „by which a person (or group) makes himself more or less accessible and open to others“[185] und als „selective control of access to the self or to one's group.“[186] Dabei betrachtet er aber ausschließlich sehr kleine soziale Einheiten, „which can include the family, a pair of people, or other small social groups.“[187] Umfassend stellt Altman dann die Mechanismen dar, mit denen Individuen diesen Regulierungsprozess steuern würden.

Mitte der siebziger Jahre wurden auch von den Informatikerinnen die ersten sinnvollen Abgrenzungen zwischen *privacy* und *security* vorgenommen. So stellen Rein Turn und Willis H. Ware fest, dass *privacy* auf die Rechte des Individuums verweise, während *confidentiality* „implies that the data themselves and the information they contain must be protected, and that their use must be confined to authorized purposes by authorized people.“[188]

2.3.2 Die Anfänge der Debatte in der BRD

Ende der sechziger Jahre begann auch in der Bundesrepublik die moderne Debatte um den Datenschutz. In den ersten Jahren war sie dabei vor allem auf die Rechtsprechung und parlamentarische Kreise beschränkt.[189] Nicht der einzige, wohl aber der wirkmächtigste Versuch, die US-amerikanische Debatte in der Bundesrepublik bekannt zu machen, war Ruprecht B. Kamlahs Dissertation über das „Right of Privacy“.[190]

Neben Kamlahs Arbeit stehen zwei richtungsweisende Beschlüsse des Bundesverfassungsgerichts (BVerfG) am Anfang der deutschen Datenschutzdiskussion: der „Mikrozensus“-Beschluss 1969 und der „Scheidungsakten“-Beschluss 1970.

Der Erste Senat des BVerfG hatte zu entscheiden, ob Teile des Mikrozensusgesetzes in der Fassung vom 05.12.1960 gegen Art. 1 und Art. 2 GG verstoßen, weil die Verpflichtung zur Beantwortung von Fragen über Urlaubs- und Erholungsreisen nach Ansicht des Amtsgerichts Fürstenfeldbruck die Intimsphäre der Befragten verletzte. Das BVerfG entschied am 16.07.1969, dass die Regelungen im Mikrozensusgesetz „weder gegen Art. 1 Abs. 1 und Art. 2 Abs. 1 GG noch gegen andere Bestimmungen des Grundgesetzes“[191] verstießen. Gleichwohl setzte das Gericht Grenzen: Weil das Grundgesetz der einzelnen Bürgerin einen unantastbaren Bereich privater Lebensgestaltung gewähre, der der Einwirkung der öffentlichen Gewalt entzogen sei,[192] widerspreche es der menschlichen Würde, den Menschen zum bloßen Objekt im Staat zu machen.[193]

> „Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität

[185] Altman (1975, S. 3).
[186] Altman (1975, S. 18).
[187] Altman (1975, S. 2). Diesen Aspekt übersehen so gut wie alle neueren Vertreterinnen dieser Theorie und wenden sie stattdessen auf *alle* sozialen Beziehungen an, also etwa auch auf solche zwischen Individuen und Organisationen. Diesen Prozess des Oszillierens zwischen Öffnung und Abgrenzung bezeichnet Altman falsch als „dialektisch“, was scharfe Kritik hervorrief, siehe etwa Foddy (1984). Aber auch diese Zuschreibung wird bis heute wiederholt.
[188] Turn und Ware (1975, S. 7).
[189] Vgl. Giloi (1970, S. 9).
[190] Kamlah (1969).
[191] BVerfG (1969, S. 5).
[192] Siehe (BVerfG, 1957, S. 41).
[193] Siehe BVerfG (1956, S. 204).

> einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.“[194]

Im Zusammenhang mit statistischen Befragungen führte das Gericht aus:

> „Eine statistische Befragung zur Person kann deshalb dort als entwürdigend und als Bedrohung des Selbstbestimmungsrechtes empfunden werden, wo sie den Bereich menschlichen Eigenlebens erfaßt, der von Natur aus Geheimnischarakter hat, und damit auch diesen inneren Bezirk zu statistisch erschließbarem und erschließungsbedürftigem Material erklärt.“[195]

Weil die Befragung zu Urlaubs- und Erholungsreisen weder zur Offenlegung der Intimsphäre zwinge noch die einzelnen Details Geheimnischarakter besäßen und sich alle Daten auch ohne die Betroffenen ermitteln ließen, sei die Menschenwürde nicht beeinträchtigt und daher sei das Mikrozensusgesetz verfassungsgemäß. Das Urteil steht noch ganz in der Tradition der Sphärentheorie, verweist aber schon auf eine mögliche Bedrohung des Selbstbestimmungsrechtes durch die staatliche Informationserhebung.

Ein gutes halbes Jahr später, am 15.01.1970, fällte der gleiche Senat des BVerfG den „Scheidungsakten“-Beschluss. Gegen einen im Ruhestand befindlichen Oberstadtdirektor wurde ein Disziplinarverfahren wegen des Verdachts der Unterhaltung eines „ehebrecherischen Verhältnisses“ durchgeführt. Der Untersuchungsführer im Disziplinarverfahren erbat im Wege der Rechts- und Amtshilfe bei der zuständigen Zivilkammer die Akten aus dem Ehescheidungsverfahren des Beschuldigten zur Einsichtnahme, die ihm auch – ohne Kenntnis oder Einwilligung des betroffenen Ehepaares – gewährt wurde. Nachdem der Betroffene von dem Vorgang Kenntnis erhalten hatte, klagte er vor dem Oberlandesgericht (OLG) Hamm gegen die Herausgabeverfügung. Die Klage wurde abgewiesen, der Betroffene machte vor dem BVerfG die Verletzung seiner verfassungsmäßigen Rechte geltend. Das BVerfG erklärte, der Beschluss des OLG verletze den Betroffenen in seinem Grundrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG, hob den Beschluss auf und verwies die Sache zurück an das OLG Hamm.[196] Im Urteil wird zugleich der datenschutzrechtliche Erlaubnisvorbehalt definiert, nach dem personenbezogene Daten nur aufgrund von Gesetzen oder mit der Einwilligung der Betroffenen verarbeitet werden dürfen.

Kamlah äußert deutliche Kritik an den Urteilen: Weder gelinge dem BVerfG eine „brauchbare Abgrenzung eines »Intimbereichs«“, da von Natur aus nichts geheim sei, noch könne es gelingen, „gewisse »Sphären« der Geheimhaltung untereinander objektiv abzugrenzen“.[197] Er schlussfolgert, dass das Gericht die im „Scheidungsakten“-Urteil „eingangs noch aufrechterhaltene These vom »unantastbaren Kernbereich privater Lebensgestaltung« praktisch aufgegeben“ habe.[198] Abschließend setzt sich Kamlah mit den Folgen der beiden Urteile für die Einrichtung und den

[194] BVerfG (1969, S. 6).
[195] BVerfG (1969, S. 7).
[196] Siehe BVerfG (1970).
[197] Kamlah (1970, S. 362).
[198] Kamlah (1970, S. 362). Inzwischen wird der Begriff des „unantastbaren Kernbereichs privater Lebensgestaltung“ in fast allen BVerfG-Urteilen, die informationelle Sachverhalte betreffen, ausgiebig rezitiert. Der Begriff beschreibt allerdings nichts anderes als eine leere Menge. Gerade das macht es natürlich sehr einfach, ausführlich über die Eigenschaften seiner Elemente auszulassen. Einen solchen für den Staat unantastbaren Bereich kann es in einem Rechtsstaat auch gar nicht geben. Jeder Eingriff ist grundsätzlich möglich und unterliegt dabei ausschließlich den Anforderungen des Verhältnismäßigkeitsprinzips. Die faktische Grenze staatlicher Eingriffe wird nur durch die technische Machbarkeit bestimmt. Siehe beispielhaft BVerfG (1989, S. 376 f.) zur strafprozessualen Verwertbarkeit von Tagebuchaufzeichnungen: „Die Aufzeichnungen gehören nicht dem absolut geschützten Bereich persönlicher Lebensgestaltung an. Eine solche Zuordnung ist schon deshalb in Frage ge-

Betrieb „öffentlicher Datenbanken“ (Informationssysteme) auseinander: So sei etwa klar, dass „eine integrierte Datenbank mit freier Zugriffsmöglichkeit auf alle im System gespeicherten Daten verfassungswidrig“ sei, „[j]eder vorgesehene Datenaustausch [...] pränormiert werden“ müsse und der Betroffene vor einem Datenaustausch „zur Stellungnahme aufgefordert werden“ müsse.[199] Außerdem folge notwendig aus der Relativität der Geheimnisse, dass es nicht möglich sei, „bestimmte private Daten in der Art militärischer Geheimhaltungsstufen zu klassifizieren“.[200]

Vor dem Hintergrund einer zunehmenden Verbreitung von Computern und automatisierter Informationsverarbeitung in der öffentlichen Verwaltung sowie ersten Ansätzen zu einer rechtswissenschaftlichen Debatte versucht Adalbert Podlech, die Problematik öffentlicher Informationssysteme verfassungsrechtlich zu analysieren.[201] Weil erstens das Grundgesetz keine Aussagen zur Informationsverarbeitung treffe und zweitens Computer „unser privates und öffentliches Leben so grundlegend zu ändern in der Lage sind“, müsse bei der Analyse auf die Funktionen der grundlegenden Verfassungsentscheidungen zurückgegriffen werden: „z. B. Rechtsstaatlichkeit, Gewaltenteilung, Persönlichkeitsschutz, Informationsfreiheit“.[202] So stelle die Verfügungsgewalt über öffentliche Informationssysteme einen „politischen Machtfaktor erster Größe“ dar und sei geeignet „das Kräftegewicht zwischen Legislative und Exekutive zu verschieben“.[203] Zur Aufrechterhaltung der Kontrollmöglichkeiten des Parlaments müsse diesem daher grundsätzlich Zugang zu allen gespeicherten Informationen gewährt werden. Unter Verweis auf die Informationsfreiheit Art. 5 Abs. 1 Satz 1 GG habe dies grundsätzlich auch für die Öffentlichkeit zu gelten.[204] Zum Zwecke des Persönlichkeitsschutzes fordert Podlech realistische Analysen, die sowohl die technischen wie auch die sozialen Gegebenheiten einbeziehen. Dazu gehöre einerseits die Vernetzbarkeit und Vernetzung der Computer, andererseits „die Anfälligkeit sozialer Systeme [...] für die permanente Versuchung, Ziele informell, d. h. hier unter Umgehung lästiger Vorschriften zu erreichen.“[205] Dementsprechend fordert Podlech neben dem Vorliegen einer ausdrücklichen rechtlichen Ermächtigung für jeden staatlichen Zugriff auch eine „organisatorisch-technische Trennung von Unternehmern und Benutzern der Datenbanken“.[206] Die Benutzerinnen dürften dann nur in kontrollierter Weise das System nutzen – ohne physischen Zugriff. „Die die Rechte der Benutzer definierenden Rechtsvorschriften müssen als Programme der Zentraleinheit eingespeichert sein“ und veröffentlicht werden.[207]

---

stellt, weil der Beschwerdeführer seine Gedanken schriftlich niedergelegt hat. Er hat sie damit aus dem von ihm beherrschbaren Innenbereich entlassen und der Gefahr eines Zugriffs preisgegeben (vgl. Forsthoff, Der Persönlichkeitsschutz im Verwaltungsrecht, in: Festschrift zum 45. Deutschen Juristentag [1964], S. 41 [43]). Jedenfalls aber haben sie einen Inhalt, der über die Rechtssphäre ihres Verfassers hinausweist und Belange der Allgemeinheit nachhaltig berührt. Zwar befassen sie sich nicht mit der konkreten Planung oder mit der Schilderung der hier in Rede stehenden Straftat. Mit dieser Straftat ist aber der in den Niederschriften reflektierte Vorgang in einer Weise verknüpft, daß die Aufzeichnungen selbst nicht jeglichem staatlichen Zugriff entzogen sein können.“

[199] Kamlah (1970, S. 364).

[200] Kamlah (1970, S. 364).

[201] Podlech (1970).

[202] Podlech (1970, S. 473).

[203] Podlech (1970, S. 474).

[204] Podlech (1970, S. 474).

[205] Podlech (1970, S. 474), insbesondere unter Verweis auf Luhmann (1964a).

[206] Podlech (1970, S. 475). Unternehmerin sei dabei diejenige Stelle, die Verfügungsgewalt über die Technik habe.

[207] Podlech (1970, S. 475). Die Pflicht zur Veröffentlichung folge aus dem Rechtsstaatsprinzip. Lange vor Lawrence Lessig hat Podlech den Charakter von Code als Gesetz verstanden: „Werden Rechtsvorschriften mit Hilfe von EDV-Anlagen angewandt, so ist der tatsächlich geltende Text das EDV-Programm. Die Prüfung der Übereinstimmung des normativ geltenden Textes, wie er in der Umgangssprache im Gesetzblatt verkündet ist, mit dem tatsächlich geltenden Text sollte öffentlich möglich sein.“ (a. a. O.) Die Pflicht zur Veröffentlichung

Ausschließlich auf den Persönlichkeitsbereich und die Gefahren für „das Recht auf freie Entfaltung der Persönlichkeit bzw. das allgemeine Persönlichkeitsrecht“ konzentrierte sich Ulrich Seidel.[208] Zwar benutzt auch Seidel noch den Begriff der Privatsphäre, lehnt die Sphärentheorie als rechtlichen Anknüpfungspunkt aber explizit ab:

> „Die Sammlung und Speicherung personenbezogener Dateien deckt ein Problem auf, dem das Individuum in der modernen Industriegesellschaft schon seit längerem ausgesetzt ist. Der räumliche Schutzbereich hat aufgehört, das alleinige Zentrum des Privatlebens zu sein, und hat mittlerweile durch den *Datenbereich* Konkurrenz erhalten. Der persönlichkeitsrechtliche Bezug dieses Schutzbereiches liegt darin, daß ein privater Lebenstatbestand aufgezeichnet und ohne Beteiligung des Individuums beliebig reproduzierbar und über große Entfernungen übertragbar ist. [...] Die Umwelt des Einzelnen erstreckt sich somit auch auf die zahlreich über ihn angelegten und weit verstreuten Abbildungen seines Privatlebens. Diese Entwicklung läßt die der »Sphärentheorie« zugrundeliegende dialektische Auffassung von »privat« und »öffentlich« fraglich erscheinen. [...] Die Aufspaltung des Individuums in eine öffentliche und eine private Seite kann nur überwunden werden, wenn man seine sozialen Bindungen zugleich als Konkretisierung seines Anspruchs auf private Lebensführung anerkennt.“[209]

Seidel gilt mit seiner Arbeit als „Erfinder“ des informationellen Selbstbestimmungsrechts,[210] das er – ohne den Zusatz „informationell“ – als „Selbstbestimmungsrecht, Informationen vorzuenthalten oder mitzuteilen“[211] bezeichnet, und das offensichtlich eine Übernahme der *privacy*-Definition Alan Westins darstellt. Wichtiger ist seine fundierte Trennung zwischen „Datensicherungen“ und „Datenschutz“:

> „Technische Sicherungen können aber nur die Frage beantworten, wie ein vermeintlich berechtigter Benutzer mit Gewißheit erkannt und die Ausübung seiner Rechte kontrolliert werden kann. Sie lassen das Problem offen, nach welchen Kriterien der Benutzer berechtigt sein soll, auf die gespeicherten Daten zuzugreifen.“[212]

Solche materiellrechtlichen Kriterien gebe es bisher noch nicht, auch nicht in anderen Ländern. Alle Regelungen und Regelungsentwürfe beschränkten sich auf Datensicherungsmaßnahmen.[213] Weil Informationen „im kommerziellen Bereich zur Ware werden und auf staatlicher Ebene einer perfekten Überwachung dienen“ könnten, sei „wie im amerikanischen Recht jedes personenbezogene Datum als schutzfähig anzusehen.“[214]

Auch im ersten Lehrbuch für das gerade neu entstandene Fach Rechtsinformatik findet sich ein kurzer Abschnitt zum Datenschutz.[215] In einer noch sehr oberflächlichen Form versucht Wilhelm Steinmüller, auf wenigen Seiten das Thema zumindest begrifflich abzubilden. Im Mittelpunkt steht dabei noch der Schutz der „Privatsphäre“: „Die Verwaltungsautomation und

solle auch für alle Programme gelten, mit denen personenbezogene Informationen verarbeitet werden. Siehe dazu viel später auch Köhntopp et al. (2000) und Schallaböck (2009).

[208] Seidel (1970).
[209] Seidel (1970, S. 1582), Hervorhebung im Original.
[210] Siehe von Lewinski (2014, S. 4).
[211] Seidel (1970, S. 1582 f.).
[212] Seidel (1970, S. 1583).
[213] Seidel (1970, S. 1583).
[214] Seidel (1970, S. 1583).
[215] Steinmüller (1970).

besonders die Errichtung universaler staatlicher Informationssysteme können die Privatsphäre des Bürgers durch »Computermißbrauch« bedrohen. Diese Gefährdung verlange besondere Vorkehrungen zum Schutz dieser Privatsphäre: den »Datenschutz«."[216] Wie bei Seidel ist die Definition – auch wenn Steinmüller das nicht offenlegt – von Westin übernommen: „»Recht auf Privatsphäre« sei die Befugnis zu bestimmen, ob und wieweit Dritte (Staat oder Privatpersonen) private Informationen über den Berechtigten erfassen, speichern, verarbeiten und/oder weitergeben dürfen."[217] „Computermißbrauch" soll die „negativen Folgen der Einführung staatlicher Informationssysteme und der Verwaltungsautomation" umfassen und stelle einen Sonderfall des allgemeinen Persönlichkeitsrechts dar, „der wohl gesetzlicher Regelung bedarf, da der Schutz aus GG Art. 1, 2 allein nicht ausreichen dürfte."[218] Steinmüller unterteilt die Datenschutzmaßnahmen in technische und juristische, wobei er bei den technischen Maßnahmen zwischen „input controls" und „output controls" unterscheiden will.[219] Als juristische Sicherungen verlangt er u. a. Anmeldepflichten für Datenbanken, Betroffenenrechte, die Einführung eines unabhängigen Datenschutzbeauftragten, die Beschränkung der Amtshilfe und eine Zweckbindung, abgesichert durch Strafvorschriften.[220] Auch müssten private Informationssysteme gesetzlich geregelt werden, „zumal sie [...] unschwer von Behörden benützt und so zur Umgehung etwaiger Beschränkungen benützt werden können."[221]

Im Rahmen der Formulierung des „Großen Hessenplans" wurde als Ziel für den Zeitraum bis 1980 ausgegeben, dass die Verwaltung „eine funktionsgerechte Struktur erhalten und ihre Arbeitsweise der modernen technischen Entwicklung anpassen [muss]. Die Möglichkeiten der elektronischen Datenverarbeitung müssen voll ausgeschöpft werden."[222] Gleichzeitig müsse „der Gefahr technokratischer Herrschaftsformen, die im Zusammenhang mit dieser Entwicklung aufkommen können", begegnet werden.[223] Das diesem Zweck dienende Gesetz – das „Datenschutzgesetz"[224] (HDSG) – enthielt jedoch keine Datenschutz-, sondern nur Datensicherheitsregelungen.[225] Einzig die Regelungen der Aufgaben der Datenschutzbeauftragten, die damit erstmals institutionalisiert wurde, weisen über klassische Datensicherheitsmaßnahmen hinaus: einerseits konnte sie „Vorkehrungen zur Verbesserung des Datenschutzes" anregen (§ 10 Abs. 1), andererseits war es ihre Aufgabe, „die Auswirkungen der maschinellen Datenverarbeitung auf die Arbeitsweise und Entscheidungsbefugnisse der [...] Stellen dahingehend [zu beobachten], ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen Selbstverwaltung führen" (§ 10 Abs. 2).

Auf dem 48. Deutschen Juristentag in Mainz vom 22. bis 25.09.1970 fand eine vielbesuchte Sonderveranstaltung zum Thema „Datenverarbeitung im Recht" statt. Spiros Simitis, der an

[216] Steinmüller (1970, S. 86). Steinmüller hält aber „Informationsschutz" für besser (S. 87).
[217] Steinmüller (1970, S. 87).
[218] Steinmüller (1970, S. 87).
[219] Steinmüller (1970, S. 88). Hier wird deutlich, dass Steinmüller anfangs noch eher ein Maschinenmodell des Datenschutzes vertrat, von dem er bereits kurz darauf Abstand nahm. Neben k-Anonymität beim „output" fordert er etwa auch Protokollierung sowie die „technische Absicherung der juristischen Sicherungen überhaupt" (a. a. O.).
[220] Steinmüller (1970, S. 88).
[221] Steinmüller (1970, S. 89).
[222] Hessische Zentrale für Datenverarbeitung (1970, S. 76).
[223] Hessische Zentrale für Datenverarbeitung (1970, S. VI).
[224] Hessen (1970).
[225] „Inhalt des Datenschutzes" war nach § 2 sicherzustellen, dass Informationen „nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können." Nach § 3 hatten Befugte Vertraulichkeit zu wahren.

der Formulierung des Hessischen Datenschutzgesetzes mitgewirkt hatte und später als der Doyen des Datenschutzes bezeichnet werden sollte,[226] sprach dort über die Notwendigkeit eines Datenschutzes gerade auch vor dem Hintergrund seiner gleichzeitig erhobenen Forderung nach einer „volle[n] Ausnützung der Möglichkeiten der Datenverarbeitung“. Zu schützen seien dabei sowohl die Individuen als auch die Gesellschaft als Ganze. Es gelte unter anderem zu verhindern, dass die elektronische Datenverarbeitung zu einem „Instrument einseitig gesteuerter Information“ werde.[227]

Das Potential zur Entwicklung eines solchen Instruments bestand dabei durchaus. So wurde – in Anlehnung an das „National Data Center“ der USA – in der Bundesrepublik ein „allgemeines arbeitsteiliges Informationsbankensystem“ geplant.[228] In einer ersten Analyse solcher staatlichen Informationssysteme stützt sich Steinmüller auf grundlegende modelltheoretische Überlegungen: „als Modell in bezug auf das, was es abbildet [...], in bezug auf seinen Zweck [...] und schließlich in bezug auf seine Hauptbenutzer“.[229] Mit dem Aufbau eines „dichte[n] Netz[es] von miteinander vermaschten Informationssystemen“ werde ein Modell der Bevölkerung erzeugt, das „das sogenannte Original für einen bestimmten Zweck und für bestimmte Benutzer“ simuliere. „Damit wird die Bevölkerung insoweit transparent und berechenbar; sie wird experimentierfähig.“[230] „Die potentiell völlige Erfassung der Bevölkerung gibt dem untersuchenden Modellsubjekt (z. B. einer Regierung) wissenschaftlich zuverlässige Informationen, etwa zur Beeinflussung in einem gewünschten Sinn, [sic!] oder zur Aussonderung bestimmter Volksgruppen, z. B. Juden.“[231] Ein Datenschutzgesetz, dass nur dem „individuelle[n] Schutz der Privatsphäre“ diene, biete keinen Schutz. Gefordert sei „auch und vor allem Minderheitenschutz“.[232] Steinmüllers bis heute wichtigste Feststellung lautet:

> „Es gibt keine neutrale (zweck- und benutzerunabhängige) Information.“[233]

Auch Herbert Auernhammer, der als Ministerialrat im Bundesministerium des Innern (BMI) Referent für das Recht der Datenverarbeitung und zuständig für die Ausarbeitung des Bundesdatenschutzgesetzes war, nimmt die Absehbarkeit der Einführung allgemeiner „Verbund- und Informationssysteme“ für seine Analyse der „Gefahren für die Privatsphäre“ und mögliche Lösungsansätze als gegeben an.[234] So schließt er eine Beschränkung auf automatisierte Informationsverarbeitungsvorgänge ebenso aus wie eine Nichtregelung der privaten Informationsverarbeitung. Gerade um zu verhindern, dass sich öffentliche Stellen privater Datenverarbeiter bedienen, um datenschutzrechtliche Beschränkungen zu umgehen, müsse „die Privatsphäre in beiden Bereichen gleichermaßen geschützt“ werden.[235] Als zentrales Problem sieht Auernhammer die „sog. Privacy-Problematik, also die Bestimmung des geschützten Rechtsgutes“.[236] Dabei hält er

[226] Siehe Bygrave (2008, S. 15).
[227] Weber (1970, S. 649).
[228] Siehe Hölder (1971). Das Projekt wurde 1974 öffentlich wieder abgekündigt, so Hoffmann (1979, S. 91).
[229] Steinmüller (1971c, S. 81).
[230] Steinmüller (1971c, S. 82).
[231] Steinmüller (1971c, S. 82). Siehe dazu umfassend Aly und Roth (1984).
[232] Steinmüller (1971c, S. 83).
[233] Steinmüller (1971c, S. 85). Siehe zur Einordnung in den größeren Rahmen einer entstehenden Rechtsinformatik Steinmüller (1971b), der auch explizit darauf verweist, dass der Rechtsinformatik – und mithin dem Datenschutzrecht, das ein Teil davon ist – ein Informationsbegriff zugrunde liegen muss, der nicht nur den syntaktischen, sondern ebenso den semantischen und den pragmatischen Aspekt umfassen muss (S. 3).
[234] Auernhammer (1971).
[235] Auernhammer (1971, S. 26).
[236] Auernhammer (1971, S. 26).

sowohl eine Legaldefinition der Privatsphäre als auch den „umgekehrte[n] kasuistische[n] Weg einer Einzelerfassung aller in Betracht kommenden Sachverhalte“ wegen der „Relativität der Privatsphäre“ für unmöglich.[237]

Im Dezember 1971 brachte die Interparlamentarische Arbeitsgemeinschaft einen Gesetzentwurf zu einem Bundesdatenschutzgesetz – „zum Schutz vor unbefugter Verwendung personenbezogener Daten“ – in den Deutschen Bundestag ein,[238] nachdem sie schon im Januar 1970 einen Entwurf für ein Datenüberwachungsgesetz[239] vorgelegt hatte.[240] Der Gesetzentwurf folgte weitgehend dem Vorbild des HDSG, jedoch unter Hinzunahme der „herkömmlichen“ Datenverarbeitung.[241] Ziel des Gesetzes war es, „[n]achteiligen Auswirkungen des Einsatzes der elektronischen Datenverarbeitung vorzubeugen“.[242] Gewährleistet werden sollte dies durch umfangreiche Betroffenrechte, einen Zugriffsschutz gegen Unberechtigte, den Vorbehalt des Gesetzes und die Ablehnung einer Einheit der Verwaltung.[243] Zusätzlich wird das BMI in § 28 Abs. 2 ermächtigt, durch Rechtsverordnung zu regeln, „welche Vorkehrungen zu treffen sind, um unter Berücksichtigung der wirtschaftlichen Belastbarkeit und bei Beachtung der Kenntnisse des jeweils neuesten Standes der technischen Entwicklung den in § 5 Abs. 3 und § 13 Abs. 4 auf personellem und technischem Gebiet des Datenschutzes aufgestellten Erfordernissen zu genügen.“ Während öffentliche Stellen bei der verpflichtenden Anmeldung von Datenbanken nachweisen müssen, welche Maßnahmen sie getroffen haben, müssen nicht-öffentliche Stellen nur nachweisen, dass sie Maßnahmen getroffen haben.

Nach Podlech beschäftigt sich auch Kamlah ausführlich mit dem Informationsverhältnis zwischen Parlament und Regierung sowie Verwaltung in der sich entwickelnden Informationsgesellschaft, in dem das Parlament vom enteilenden Ausbau von Informationssystemen durch die Exekutive in einer „Informationskrise“ zurückgelassen wird, durch die sich der Informationsvorsprung der Exekutive gegenüber der Legislative und damit deren Macht konträr zu den

[237] Auernhammer (1971, S. 26). Das Argument hat er wahrscheinlich von Steinmüller und Bernd Lutterbeck übernommen, die es zur Grundlage ihres grundlegenden Gutachtens machten, dass sie in Grundzügen Anfang 1971 im BMI vorstellten. Siehe dazu auch Rost und Krasemann (2009). Daher überrascht es auch nicht, dass der Younger-Report im Jahr darauf eingestehen musste, keine Definition für „privacy“ vorlegen zu können, siehe Younger (1972).

[238] Hirsch et al. (1971).

[239] Sowohl der Name wie auch der Inhalt stimme weitgehend mit dem Vorschlag für ein *Data Surveillance Bill* überein, das im Mai 1969 im britischen Unterhaus eingebracht wurde, so Steinmüller (1970, S. 86).

[240] Zeitgleich soll es im Bundesministerium des Innern einen ersten Referentinnenentwurf eines Bundesdatenschutzgesetzes gegeben haben, siehe BT-Drs. VI/3826, S. 1.

[241] Siehe in der Begründung, S. 11: „Die Computertechnik ist allenfalls der Anlaß, nicht jedoch der tiefere Grund für den Erlaß eines solchen Gesetzes.“

[242] Hirsch et al. (1971, S. 8). Die Autorinnen stützen sich dabei auf Ausführungen sowohl in der amerikanischen Debatte – Hearings (89th/2nd (1966), 90th (1967/68)), Westins „Privacy and Freedom“ (1967), Millers „Personal Privacy in the Computer Age“ (1969), Warner und Stones „The Data Bank Society“ (1970) – als auch aus der deutschen – „Mikrozensusurteil“ [sic!] (BVerfG (1969)) und Scheidungsaktenurteil (BVerfG (1970)), Kamlahs „Right of Privacy“ (1969), Seidels „Persönlichkeitsrechtliche Probleme. . . “ (1970), Simitis’ „Informationskrise des Rechts. . . “ (1970), Steinmüllers „EDV und Recht“ (1970) und Podlechs „Verfassungsrechtliche Probleme öffentlicher Datenbanken“ (1970).

[243] Mit § 8 Abs. 2 des Entwurfs wird, wie in der Begründung auf S. 12 ausgeführt, der Auffassung entgegengetreten, dass es eine solche Einheit der Verwaltung gebe, d. h. „daß unter dem Motto der Amtshilfe Behörden untereinander Daten austauschen dürften, auch wenn es sich um personenbezogene Daten handelt. Diese Auffassung ist unter zunehmenden rechtsstaatlichen Erfordernissen nicht mehr aufrechtzuerhalten. Es mehren sich die Stimmen, die in der Datenermittlung uns Datenweitergabe einen Eingriff gegenüber dem Bürger sehen. Die Amtshilfe ist lediglich eine Rechtsgrundlage gegenüber der angegangenen Behörde, Hilfe zu leisten. Sie deckt nicht den in der Amtshilfe möglicherweise liegenden Eingriff gegenüber dem Bürger.“

verfassungsrechtlichen Vorgaben strukturell vergrößert und sich nur durch die Verrechtlichung eines Informationsanspruchs des Parlaments verfassungskonform lösen lasse.[244]

In einem von Siemens herausgegebenen Band zu „Datenschutz – Datensicherung“ vertritt Jochen Schneider in den ersten beiden Kapiteln noch die traditionellen Vorstellungen von einer zu schützenden Privatsphäre, vor allem basierend auf den Arbeiten Alan Westins mit seinen vier Funktionen der Privatsphäre: „persönliche Autonomie, Gefühlsentspannung, Selbsteinschätzung und geistiges Distanzhalten (Kommunikation mit Vorbehalten)“.[245] Gleichzeitig jedoch – und eigentlich im Widerspruch zueinander und zu diesen Vorstellungen – bezieht sich Schneider auch auf die Konzeptionen der soziologischen Rollentheorie und Hubmanns Sphärentheorie.[246] Diese Fixierung auf die Privatsphäre wird von Steinmüller im Anschluss als untauglich angegriffen.[247] Datenschutz – und das gilt dann auch sowohl für die Datenschutzdiskussion als auch für das Datenschutzrecht – als „Menge aller Vorkehrungen zur Verhinderung unerwünschter Datenverarbeitung“[248] müsse nicht von einem solch „überholten“ Bild der Privatsphäre ausgehen, sondern von der „gesellschaftlichen Wirklichkeit“, die gekennzeichnet ist „von der weitgehenden Verflechtung – und gelegentlich Verfilzung – von Gesellschaft, Staat, Wirtschaft, Individuum, gesellschaftliche [sic!] Gruppierungen aller Art“.[249] Steinmüller trennt dann zwischen „Datenschutz im weiteren Sinne“ und „Datenschutz im engeren Sinn“.[250] Ersterer beschäftigt sich mit der „Gefährdung eines Informationsgleichgewichts durch Informationsmonopole“ und der „rechtspolitisch unerwünschte[n] Datenverarbeitung außerhalb der sog. Privatsphäre“, also solcher, „die gegen die Grundentscheidungen des Grundgesetzes verstößt“ wie etwa dem Prinzip der Gewaltenteilung. Dazu fordert Steinmüller die Einführung einer „behördeninternen Gewaltenteilung“, ein Prinzip, das heute als „informationelle Gewaltenteilung“ bezeichnet wird. Für den Datenschutz im engeren Sinne stellt Steinmüller fest, dass sowohl die Trennung zwischen Personen- und Sachdaten als auch die Trennung von individuellen und statistischen Daten relativ seien und daher alle Daten dem Datenschutz unterfallen müssten. Abschließend zieht er aus den „Erwägungen über den Charakter von Daten“ Forderungen für die Institutionalisierung des Datenschutzes.[251] Christoph Mallmann beschäftigt sich in seinem Beitrag mit dem Individualdatenschutz, d. h. dem Datenschutz im engeren Sinne.[252] Als unerwünscht im Sinne der Definition Steinmüllers bezeichnet er „Machtmißbrauch oder bereits die Möglichkeit zum Machtmißbrauch“:

> „Nun ist es ohne weiteres einsichtig, daß die potentiellen Mißbrauchsmöglichkeiten des Staates davon abhängen, wieviel und welche Daten dem Staat über seine Bürger zur Verfügung stehen. Will man also die Mißbrauchsmöglichkeiten herabsetzen, so muß man die Verfügungsmöglichkeiten des Staates beschränken.“[253]

Mallmann kritisiert die Art und Weise der durch Kamlahs Arbeit in der Bundesrepublik entfachten Diskussion als „auf Probleme des Einzelbürgers verengt“ und durch „die vorschnelle Über-

[244] Kamlah (1971b); Kamlah (1971c).
[245] Schneider (1971, S. 8).
[246] Schneider (1971, S. 9).
[247] Steinmüller (1971a).
[248] Steinmüller (1971a, S. 13).
[249] Steinmüller (1971a, S. 14).
[250] Steinmüller (1971a, S. 14 ff.). Bernd Lutterbeck wird später behaupten, nur der Datenschutz im engeren Sinne sei vom einfachen Gesetzgeber regelbar, während der Datenschutz im weiteren Sinne nur im Grundgesetz geregelt werden könne, siehe Lutterbeck (1976, S. 170).
[251] Es handelt sich dabei um eine Wiederholung dessen, was Steinmüller und seine Mitautorinnen in den „Grundfragen des Datenschutzes“ behandeln.
[252] Mallmann (1971).
[253] Mallmann (1971, S. 19).

setzung von »privacy« in Privatsphäre“ in eine falsche (und veraltete) Richtung gezogen.[254] Ausgehend von verschiedenen in der Diskussion vorgebrachten Definitionen von Privatsphäre versucht Mallmann zu zeigen, dass es unmöglich sei, „von einem bestimmten personenbezogenen Datum von vornherein – also ohne Einbeziehung des Betroffenen – festzustellen, ob es zur Privatsphäre gehört oder nicht.“[255] Im Ergebnis fordert er, den Begriff der Privatsphäre in der Debatte fallen zu lassen, und dass der Datenschutz sich auf den „gesamte[n] Lebensbereich einer Person [beziehen müsse], innerhalb dessen Daten über diese Person in irgendeiner Weise verfügbar sind.“[256] Das daraus entstehende „Recht auf Schutz der »Privatsphäre«“ teilt Mallmann in ein passives Recht – „ein Recht des Einzelnen auf Schutz des Persönlichkeitsbereiches, der ihn zum Zusammenleben befähigt“ – und ein aktives Recht – „das Recht, das Bild, das sich die Umwelt von ihm macht, selbst zu steuern, d. h. eine bestimmte Rolle zu spielen.“[257] In den nachfolgenden Kapiteln führt Schneider in die Datensicherung ein und stellt Inhalt und Zwecke von Datenschutz und Datensicherung einander gegenüber.[258] In dem Versuch, den Umgang mit Missbrauch (im Sinne Steinmüllers und Mallmanns) darzustellen, unterscheidet Schneider zwischen „Geheimhaltung“ und „Empfindlichkeit“, wobei er die Geheimhaltung „als Interesse des Verwalters der Dateien und Interesse der Organisation, die die Datenverarbeitungsanlage unterhält“ bezeichnet und auf den amerikanischen Begriff der „security“ abbildet. Mit der Empfindlichkeit bezeichnet er das „Interesse der durch die Daten erfaßten Personen“ und sieht es gleichbedeutend mit der amerikanische Bezeichnung „sensitivity“.[259]

Während seine Arbeiten zu Webers Bürokratietheorie,[260] zur Organisationswissenschaft,[261] zu Grundrechten,[262] zur Verwaltungswissenschaft im Allgemeinen,[263] zur Verwaltungsautomation im Besonderen[264] und zur soziologischen Systemtheorie[265] in weitem Umfang die Grundlage für Beschreibung und Erklärung der gesellschaftlichen Informationsverarbeitung, ihrer Bedingungen und ihrer Folgen waren, hat Niklas Luhmann nur ein Mal selbst Überlegungen zum Datenschutz veröffentlicht – und diese „beschränken sich auf den Organisationsteil der Verfassung“.[266] Sein Hauptaugenmerk liegt dabei auf den Folgen der Automation für das Ressortprinzip als Aspekt der Gewaltenteilung. Mit den Folgen für die horizontale und vertikale Gewaltenteilung in ihrer Gesamtheit beschäftigen sich Malte von Berg, Uwe Harboth, Hans D. Jarass und Bernd Lutterbeck:

> „Es besteht die Gefahr, daß die auch dem Schutz von Freiheitsräumen dienende Differenzierung des Staatsapparats in Zuständigkeiten, Kompetenzen usw. zugunsten größerer Effektivität von Verwaltung und Regierung aufgegeben werden und die Vorteile einer machthemmenden Staats- und Verwaltungsorganisation verschwinden.“[267]

[254] Mallmann (1971, S. 21).
[255] Mallmann (1971, S. 23).
[256] Mallmann (1971, S. 24).
[257] Mallmann (1971, S. 25) unter Rückgriff auf die soziologische Rollentheorie.
[258] Schneider (1971, S. 40 f.).
[259] Schneider (1971, S. 62). Diese Trennung der unterschiedlichen Interessen bleibt in der Debatte oft unbeachtet. Sie ist aber notwendig, um eine falsche Gleichsetzung von Sicherheit und Datenschutz – und der daraus folgenden Fehlannahme, dass IT-Sicherheitsmaßnahmen zugleich Datenschutzmaßnahmen seien – zu verhindern.
[260] Siehe etwa Luhmann (1964b).
[261] Siehe etwa Luhmann (1964a), Luhmann (1977), Luhmann (1969).
[262] Siehe etwa Luhmann (1986).
[263] Luhmann (1966b).
[264] Siehe etwa Luhmann (1966a).
[265] Siehe etwa Luhmann (1966a).
[266] Luhmann (1972).
[267] von Berg et al. (1972, S. 4).

Eine inhaltliche Kontrolle besitze dabei funktionelle Schwächen: Einerseits komme es zu einer Problemverschiebung von der Kontrolle auf die Kontrolle der Kontrolle oder die Kontrolle des Kontrollorgans, andererseits wirke die inhaltliche Kontrolle verschleiernd, da es schlicht zu viele Möglichkeiten des Machtmissbrauchs gebe, als dass sie alle kontrolliert werden können.[268] Gelöst werden könne dieses Problem der Machtkontrolle daher nur durch strukturelle Maßnahmen, die gleichzeitig stärker präventiv wirken: durch Schaffung eines Informationsgleichgewichts gegen die informationsmonopolistischen Tendenzen von Regierung und Verwaltung zugunsten von Parlament, Opposition und Öffentlichkeit.[269]

In seiner Dissertation, mit der er seine früheren Positionen teilweise verschärft, kritisiert Seidel sowohl die Sphären- als auch die Mosaiktheorie des Persönlichkeitsrechts.[270] Stattdessen spricht er sich unter Zuhilfenahme der Zustandstheorie Westins für einen sphären- *und* zustandsorientierten Persönlichkeitsschutz aus, wobei letzterem die dominierende Rolle zukomme.[271] Als einer der Ersten verlangt er, originäre Datenschutzanforderungen technisch umzusetzen: So müsse bei Sekundärdaten immer auch die Herkunft gespeichert werden, „um den Datenweitergebenden jederzeit identifizieren zu können." Auch müsse bei der Dateneingabe gleichzeitig die Löschfrist erfasst werden, damit automatisiert gelöscht werden kann.[272]

Nachdem Luhmann die von Dahrendorf nach Deutschland importierte[273] soziologische Rollentheorie für das Recht salonfähig gemacht hatte[274] und diese von Schneider schon – wenn auch noch sehr oberflächlich – in den Datenschutzdiskurs eingebracht worden war,[275] versuchten sich Paul J. Müller und H. H. Kuhlmann an einer ersten fundierten Anwendung der Rollentheorie zur theoretischen Analyse des Datenschutzproblems. Sie beschreiben das Datenschutzproblem als „the »visibility« of individuals, or the »transparency« of their features consequent on the widespread establishment of feature-profiles."[276] In Abgrenzung zu anderen soziologischen Definitionsversuchen von *privacy*[277] stützen sie sich nicht auf eine absolute Konzeption von *privacy*, sondern eine kontextspezifische: *Privacy* ist „the individual's »visibility« in varying contexts",[278] „the role-specific exclusivity of the information".[279] Aus dieser Sicht würden integrierte Informationssysteme die Gefahr einer einseitigen Änderung des Verhältnisses zwischen Individuum und Organisation hervorbringen – Individuen werden für Organisationen transparent, während die Organisationen für die Individuen weiterhin intransparent bleiben – und mithin zu einer Verschiebung der Macht zugunsten der Organisationen führen.[280] Obwohl in einer renommierten

[268] von Berg et al. (1972, S. 6).
[269] von Berg et al. (1972, S. 6 f.). Die Autoren fordern dabei sowohl ein eigenständiges Parlamentsinformationssystem wie auch die Publizität staatlicher Daten – heute wieder unter dem Stichwort »Open Data« diskutiert – und darüber hinaus ein „übergreifendes Gesellschafts-Informationssystem mit autonomen Teilbereichen".
[270] Seidel (1972, S. 66 ff.).
[271] Seidel (1972, S. 68 ff.).
[272] Seidel (1972, S. 167 ff.). Beide Forderungen beschreiben, was heute als „sticky policies" diskutiert und damals wahrscheinlich von Miller – Miller (1971, S. 144) – in die Diskussion eingeführt wurde.
[273] Siehe Dahrendorf (1965).
[274] Luhmann (1986). Luhmann hat dabei vor allem die strukturalistische Rollentheorie-Strömung von Talcott Parsons (1951) und Robert K. Merton (1949) übernommen, nicht die interpersonale von Erving Goffman (1956 und 1959).
[275] Schneider (1971).
[276] Müller und Kuhlmann (1972, S. 585).
[277] Die Autoren verweisen etwa auf soziologische *privacy*-Definitionen von Paul Halmos, Arnold Simmel, Alan F. Westin und Erwin K. Scheuch.
[278] Müller und Kuhlmann (1972, S. 590).
[279] Müller und Kuhlmann (1972, S. 595).
[280] Müller und Kuhlmann (1972, S. 596).

internationalen Fachzeitschrift erschienen, ist auf den Artikel in der späteren *privacy*-Debatte nicht mehr eingegangen worden, selbst dort nicht, wo es Bezüge zur Rollentheorie zu ziehen gab oder gegeben hätte. Insbesondere Müller hat diese soziologische und rollentheoretische Konzeption von Privatheit später weiter ausgearbeitet: „Privatheit wird dann in Lebensbereichen möglich, in denen Individuen qua spezifischen Rollen agieren und in denen die Wahrscheinlichkeit gering ist, daß Informationen über sie an einen anderen Lebensbereich weitergegeben werden.“[281] Schutzziel sei demnach die rollenspezifische Exklusivität von Informationen.[282]

Die Diskussion in der Bundesrepublik war in den Siebzigern stark eingebettet in eine europaweite Diskussion. Zu den Personen, die über ihre Landesgrenzen hinweg Einfluss auf die Datenschutzdiskussion nahmen, gehörte zweifellos Kerstin Anér, die als schwedische Parlamentarierin Mitglied des Committee on Data Industry war und zu den wichtigsten Datenschutzevangelistinnen Schwedens gehörte. Von ihr stammen sowohl das bis heute verwendete Bild der „goldfish bowl“ für die verdatete Gesellschaft als auch das noch sehr viel präsentere „data-shadow“ für das Verdatungsmodell des Individuums, das „often [will] be taken for himself, and he will have to pay for all its inaccuracies as if they were his own“, obwohl letzteres heute vielfach fälschlicherweise Alan Westin zugeschrieben wird.[283] Die Antwort darauf müsse lauten: „control the controller, manipulate the manipulators and share the information power as widely as possible.“[284] Einen Teil dieser Debatte hat Frits Hondius Mitte der 1970er Jahre zum Gegenstand einer vergleichenden Untersuchung gemacht, aber leider nur einen sehr kleinen Teil davon: die Gesetze und Gesetzentwürfe.[285]

Neben den bereits angesprochenen Topoi Gewaltenteilung und individueller Selbstdarstellung verweist Podlech unter Rückgriff auf Luhmann auf die besonderen Probleme, die durch die Zusammenstellung und Übermittlung von Persönlichkeitsprofilen entstehen.[286] Als Persönlichkeitsprofil will Podlech einen Datensatz über eine Person verstanden wissen, „der umfassend Auskunft über die Persönlichkeit gibt“, deren Bedrohung in der „Blockierung der Zukunft“ liege.[287]

[281] Müller (1973, S. 63).

[282] Vergl. Müller (1973, S. 64). Müller hat den Rollenbegriff dabei trotz fundierter Kritik, etwa von Frigga Haug, siehe Haug (1972), verwandt, weil er die Verwendung der sozialwissenschaftlich überholten Vorstellung der Sphärentheorie in der Diskussion überflüssig machte und dabei im konkreten Anwendungsbereich trotz der Kritik sinnvoll und produktiv angewandt werden konnte, wie er in persönlicher Kommunikation mit dem Verfasser erläuterte. Ernst Benda, unter dessen Vorsitz das Bundesverfassungsgericht 1983 das Volkszählungsurteil fällte, verwies ein Jahr später in seiner Arbeit Benda (1974) auf Müllers Ansatz in dem Versuch, die Sphärentheorie auch in der rechtswissenschaftlichen Diskussion zu überwinden, und schickte Müller seinen Beitrag mit den entsprechenden Anmerkungen zu, siehe Rost (2012a), ab Minute 41:00. Benda zitiert jedoch nicht, wie Müller im Interview behauptet, den englischsprachigen Text von 1972, sondern den in der Zeitschrift ÖVD 1973 erschienenen.

[283] Anér (1972, S. 179). Wer wann diese Fehlzuschreibung begann, lässt sich nicht feststellen, aber es könnte Garfinkel (2000, S. 70) gewesen sein, auf den nachfolgende Quellenangaben zurückgehen.

[284] Anér (1972, S. 180).

[285] Siehe Hondius (1975). Trotz dieser Beschränkung wurde und wird Hondius vor allem von Juristinnen immer wieder für Verweise auf inhaltliche Auseinandersetzungen und Entscheidungen in den Anfangsjahren der Datenschutzdiskussion verwendet, selbst für die Identifizierung von Fehlstellen in der Diskussion. Siehe dazu etwa beispielhaft die Dissertation von Gloria González Fuster (2014) zur Entstehungsgeschichte eines europäischen Grundrechts auf Datenschutz.

[286] Siehe Podlech (1972).

[287] Podlech (1972, S. 157). Er zitiert dazu Luhmann mit „In der Gegenwart müssen jetzt Unbestimmtheiten bereit gehalten werden, die sich erst durch künftige Dispositionen ausfüllen lassen, oder Bestimmtheiten, die auf spätere Umdeutung hin angelegt sind.“ Es geht hier also um die Aufrechterhaltung von Kontingenz, mithin von Entscheidungsfreiheit über die Zukunft. Trotzdem ist die Annahme, um ein Persönlichkeitsprofil handele es sich

2.3.3 Die Gutachten zum Datenschutz

Im September 1972 wurden die drei vom BMI in Auftrag gegebenen Datenschutzgutachten nach langer Weigerung als Bundestagsdrucksache veröffentlicht: die „Grundfragen des Datenschutzes“ von Steinmüller und seinen Mitarbeiterinnen[288], Kamlahs Arbeit „Datenschutz im Spiegel der anglo-amerikanischen Literatur“[289] und die „Überlegungen zu technischen Möglichkeiten des Datenschutzes im Hinblick auf ein Bundesdatenschutzgesetz“ von Karl Steinbuch und Herbert Wacker.[290]

Das von Steinmüller und seinen Mitarbeiterinnen[291] angefertigte Gutachten stellt eine signifikante Weiterentwicklung der theoretischen Auseinandersetzung mit dem Datenschutz dar. Während frühere Arbeiten – auch Steinmüllers eigene – noch ein Maschinenmodell der Datenverarbeitung für die Analyse und Lösung des Datenschutzproblems zugrunde legten und dabei etwa „input controls“ und „output controls“ forderten,[292] wurde nun das informationsverarbeitende System Organisation zum Ausgangspunkt der Analyse gemacht. Die Argumentationsstruktur des Gutachtens folgt grob einem Dreischritt: In einem ersten Schritt wird der Stand der gesellschaftlichen Informationsverarbeitung beschrieben. Im Mittelpunkt steht dabei die automationsgestützte Informationsverarbeitung durch Organisationen. Ergebnis der Analyse ist, dass „die IV [Informationsverarbeitung] eine typische Struktur aufweist (Struktur verstanden als regelmäßige Wiederkehr gleicher Zustände des Prozesses der IV [. . .])“: Damit ist die Phasenorientierung der Informationsverarbeitung angesprochen.[293] Die einzelnen Phasen sind dabei: „Informationsermittlung, Informationserfassung, Informationsspeicherung, Informationsveränderung, Informationsausgabe, insbesondere -weitergabe, -austausch, -verbund, [und] Informationslöschung.“[294] Im zweiten Schritt werden die zentralen Risiken beschrieben, die sich aus der aufkommenden Industrialisierung der Informationsverarbeitung insgesamt ergeben: die „Gefährdung der »Privatsphäre« des einzelnen, [und die] Gefährdung des Machtgleichgewichts.“[295] Im dritten Schritt werden dann auf der Basis des identifizierten Metamodells der organisierten Informationsverarbeitung – seiner Phasenorientierung – konkrete Gefahren, die innerhalb der einzelnen Phasen für die Grundrechte der Betroffenen entstehen können,[296] analysiert, bewertet und direkt daraus

erst, wenn es „umfassend“ Auskunft über die Person gebe, falsch. In einer modernen, funktional differenzierten Gesellschaft ist schon ein Profil in der Lage, zu einer „Blockierung der Zukunft“ zu führen, dass *nur eine Rolle* umfassend abbildet, so schon Steinmüller et al. (1971, S. 97). Und in Abhängigkeitsverhältnissen dürfte noch ein viel kleineres Profil reichen, um schon als umfassend gelten zu können. Aus Sicht der Datenverarbeiterin jedenfalls bestimmt sich die Umfassendheit eines Profils nach dem Zweck, den die Datenverarbeiterin verfolgt.

[288] Steinmüller et al. (1971). Steinmüller selbst hat 2007 eine nur teilweise überzeugende Darstellung des historischen und wissenschaftlichen Kontexts geliefert, Steinmüller (2007). Eine umfassendere Kritik findet sich in Pohle (2014a).

[289] Kamlah (1971a).

[290] Steinbuch und Wacker (1972).

[291] Im Gutachten werden genannt: Bernd Lutterbeck, Christoph Mallmann, U. Harbort, G. Kolb, Jochen Schneider, Carl-Eugen Eberle, Hansjürgen Garstka, Helga Tubies. Nicht alle tauchen als Autorinnen auf, einige auch nur in einer Danksagung. Ob es sich bei U. Harbort und Uwe Harboth (siehe S. 39) um die gleiche Person handelt oder nicht, ist unklar.

[292] Siehe etwa Steinmüller (1970, S. 88).

[293] Steinmüller et al. (1971, S. 57).

[294] Steinmüller et al. (1971, S. 57).

[295] Steinmüller et al. (1971, S. 36).

[296] Diese Beschränkung der Lösungsausarbeitung auf nur einen Teil der identifizierten Problembereiche erklären die Autorinnen mit der einschränkenden Vorgabe für den Gutachtenauftrag, siehe Steinmüller et al. (1971, S. 34).

konkrete Schutzanforderungen in Form (öffentlich-)rechtlicher – und dabei vor allem formeller – Regelungen ausformuliert.

Dem Gutachten liegen mehrere Annahmen zugrunde, die nur zum Teil in der Arbeit selbst expliziert werden. Die erste Annahme betrifft den Charakter des Datenschutzes als „Kehrseite der Datenverarbeitung."[297] Unterstellt, die Annahme ist korrekt, dann folgt daraus einerseits, dass sich die Notwendigkeit des Datenschutzes nur aus dem spezifischen Charakter der gesellschaftlichen Informationsverarbeitung ableiten lässt, und andererseits, dass Datenschutz so lange gesellschaftlich notwendig ist, wie es gesellschaftliche Informationsverarbeitung gibt. Aus der zweiten Schlussfolgerung folgt dann, dass das Datenschutzproblem im grundsätzlichen Sinne nicht gelöst werden kann, sondern vor dem Hintergrund des Standes der Informationsverarbeitung gesellschaftlich immer wieder neu ausgehandelt werden muss. Diese Aushandlung kann dabei, so folgt sowohl aus der ersten Schlussfolgerung wie auch aus den Ausführungen der Autorinnen zur Notwendigkeit interdisziplinärer Zusammenarbeit bei der Analyse der gesellschaftlichen Informationsverarbeitung,[298] nicht allein den Juristinnen überlassen werden, weder damals noch heute oder in Zukunft, auch wenn die Problemlösungsansätze sehr wahrscheinlich in der Sprache des Rechts niederzulegen sind.[299]

Die zweite – und zentrale – Annahme, die der Analyse des Datenschutzes zugrunde gelegt wurde, ist die der „Unbrauchbarkeit der Privatsphäre" als Erklärungsansatz für die Analyse der Grundrechtsgefährdungen durch die Informationsverarbeitung.[300] Ausführlich geben die Autorinnen den Stand der Debatte um die Definition von Privatsphäre wieder: von einem zu schützenden Bereich des Privaten, der Unbefangenheit des gesprochenen und der Geheimhaltung des geschriebenen Wortes, den verschiedenen Geheimhaltungs- und Verschwiegenheitspflichten bis hin zum allgemeinen Persönlichkeitsrecht. Die Autorinnen kommen zu dem Schluss, dass es unmöglich sei, „die »Privatsphäre« genau zu umgrenzen und somit Verletzungen scharf feststellen zu können", und geben drei Gründe dafür an: Erstens seien die Vorstellungen extrem abhängig von Ort und Zeit und änderten sich daher stärker und schneller als andere zentrale Rechtsbegriffe. Zweitens sei „Privatsphäre" auch relativ zu seinen Trägerinnen und dem jeweiligen Gegenüber, und drittens könne eine Schutzwürdigkeit „in der Regel erst beurteilt werden [...], wenn sie bereits verletzt [sei]."[301] Dies bezeichnen sie als „Relativität der Privatsphäre". Aus dem gleichen Grunde sehen die Autorinnen kasuistische Bestimmungsversuche und Festlegungen von Schutzbereichen wie von Hubmann oder Kamlah zum Scheitern verurteilt.[302] Auch die

[297] Steinmüller et al. (1971, S. 34).

[298] Die Autorinnen verlangen direkt nach juristischer und rechtspolitischer, informatischer, system- und informationswissenschaftlicher Beteiligung, siehe Steinmüller et al. (1971, S. 34), und indirekt auch nach psychologischer, soziologischer und kybernetischer, siehe Steinmüller et al. (1971, S. 86).

[299] Das wiederum folgt aus der gesellschaftlichen Funktion des Rechts als Instrument des Ausgleichs gesellschaftlicher Interessengegensätze.

[300] Vergl. Steinmüller et al. (1971, S. 48 ff.).

[301] Steinmüller et al. (1971, S. 51). Dabei ist der zweite Grund tatsächlich der relevanteste, insbesondere dort, wo das Problem auf das Gegenüber zugespitzt wird: „Relativität der »Privatsphäre« heißt also: »Privatsphäre« gegenüber wem?" Weil die Autorinnen allerdings nur von „C" als Gegenüber sprechen, wird nicht klar, ob es sich um Personen oder um Organisationen handelt. Dabei ist gerade das ein fundamentaler Unterschied, denn Personen sind weder Gegenstand der funktionalen Differenzierung noch der Kompetenzzuweisung oder „Trägerinnen" von Eigenlogiken. Und obwohl der Bezugspunkt des Gutachtens Organisationen sind, macht die hier zutage tretende Unsauberkeit bei der Verwendung von Sprache diese Beschreibung anfällig für Anschlüsse von individualistisch-interaktionistischen Interpretationen und Theorien.

[302] Steinmüller et al. (1971, S. 52 f.). Hubmanns Unterteilung enthalte die Schutzbereiche „Recht auf Entfaltung der Persönlichkeit", „Recht an der Persönlichkeit" und „Recht auf Individualität", denen er jeweils eine Vielzahl von Einzeltätbeständen zuordne, so die Autorinnen unter Verweis auf Hubmann (1967, S. 157 ff.), während

Ersetzung der „Privatsphäre“ durch andere Termini, die weniger verschwommen sein sollen, wie „Privatheit“, „Erheblichkeit“ und „Identifizierbarkeit“ kann nach begründeter Meinung der Autorinnen nicht zum Erfolg führen: „Privatheit“ sei einerseits nicht sinnvoll von „Öffentlichkeit“ als seinem „Gegenbegriff“ abgrenzbar, weil die Grenzziehung wieder nur relativ zum Betroffenen möglich sei, und andererseits folge sie in ihrer Vorstellung eines staatsfreien Bereichs einem überkommenen Gesellschaftsbild – dem klassischen Liberalismus mit seiner Trennung zwischen Staat und Gesellschaft und dem ausschließlichen status negativus der Bürgerin.[303] Für die „Erheblichkeit“ als Abgrenzungsmerkmal ergeben sich nach Meinung der Autorinnen die gleichen Schwierigkeiten mit der Relativität wie bei der „Privatsphäre“. Sogar die „Identifizierbarkeit“ sei nur ein relatives Abgrenzungsmerkmal gegenüber „statistischen Informationen“.[304] Gerade vor dem Hintergrund der Industrialisierung der gesellschaftlichen Informationsverarbeitung ist diese Relativität und Subjektivität der „Privatsphäre“ ein fundamentales Problem für eine rechtliche Regelung, die stattdessen auf einer sinnvollen Objektivierung aufbauen muss, um die informationsverarbeitenden Organisationen angemessen klar verpflichten zu können.

Neben diesen explizit ausgesprochenen Annahmen liegen der Ausarbeitung allerdings auch nicht explizierte Annahmen zugrunde. Dabei handelt es sich erstens um jene über den Charakter der Organisationen, die von den Autorinnen als informationsverarbeitende Systeme betrachtet werden, zweitens die über den Charakter der Maschine, die in den Organisationen zur Unterstützung oder zur Übernahme von Informationsverarbeitung und Entscheidungsfindung verwendet wird, und drittens die über die Komplexität des betrachteten Informationsverarbeitungssystems. Die Autoren betrachten ausschließlich rationale Bürokratien im Sinne Max Webers, mithin also Organisationen, die sich selbst rational organisieren, die Prozesse ihrer eigenen Entscheidungsfindung rational vorplanen, die dafür notwendigen Informationsverarbeitungsprozesse in geeigneter Weise formalisieren und rationalisieren, diese dann auch gegebenfalls automatisieren und danach funktionieren wie ein Uhrwerk.[305] Zweitens unterstellen die Autorinnen dem Computer einen ausschließlich instrumentellen Charakter, den er wohl auch Anfang der Siebziger noch hatte. Mit dem Erscheinen des PC Anfang der Achtziger hat sich der Computer jedoch zu einer allgemeinen Medien- und Kommunikationsmaschine verändert und ist damit viel mehr als nur ein Werkzeug – „Denkverstärker“[306] –, das speziell auf einen konkreten Informationsverarbeitungsprozess oder sogar nur einen einzelnen Informationsverarbeitungsschritt zugeschnitten ist. Die dritte nicht explizierte Annahme der Autorinnen betrifft die Phasen der Informationsverarbeitung und den Schutz der Betroffenenrechte: Die Autorinnen versuchen, für jede Phase die möglichen Grundrechtsgefährdungen für die Betroffenen zu identifizieren und durch rechtliche

Kamlah in Anlehnung an die amerikanische Debatte die Schutzbereiche „Identitätsmerkmale“, „räumlicher Schutzbereich“, „private Daten und Tatsachen“ und „psychische Phasen der Persönlichkeit“ unterscheide, so die Autorinnen mit Verweis auf Kamlah (1969, S. 82 ff.).

[303] Vergl. Steinmüller et al. (1971, S. 53).

[304] Vergl. Steinmüller et al. (1971, S. 53 f.). Die Autorinnen geben zu, dass sie nicht wüssten, „ob die Statistikwissenschaft nicht Methoden entwickelt hat, die Rückschlüsse auf Einzelpersonen in gewissem Umfang zulassen, selbst wenn die Urdaten gelöscht sind.“ Das war zu diesem Zeitpunkt tatsächlich schon der Fall, siehe Hoffman und Miller (1973), bei dem es sich um einen Nachdruck aus der Zeitschrift Datamation von 1970 handelt.

[305] Es gibt in dem Gutachten keine einzelne Stelle, auf den verwiesen werden könnte, um zu belegen, dass die Autorinnen von rationalen Bürokratien als Organisationsform ausgingen. Was dem vielleicht am nächsten kommt, ist die Formulierung auf S. 49, nach der die betrachteten Organisationen „Integration, Automation und Rationalisierung“ anstrebten. Das ganze Gutachten atmet jedoch diesen Geist, wie selbst oberfläches Lesen nachvollziehbar macht. Wolfgang Coy, der in den Achtzigern mit Wilhelm Steinmüller an der Uni Bremen zusammenarbeitete, verwies denn auch darauf, dass es in Steinmüllers Vorstellung nur diese eine Art von Organisation gegeben habe, deren Prototypen das Preußische Militär und Siemens seien.

[306] Steinmüller et al. (1971, S. 39), in Übernahme eines Ausdrucks von William Ross Ashby.

Regelungen deren Verwirklichung zu verhindern.[307] Diesem Vorgehen liegt die Annahme zugrunde, dass Grundrechtsgefährdungen durch die Informationsverarbeitung insgesamt ausgeschlossen seien, wenn sie nur für jede Phase ausgeschlossen sind. Beim betrachteten Informationsverarbeitungssystem handelt es sich jedoch zweifellos um ein komplexes System,[308] dessen wesentliche Eigenschaft darin besteht, dass das Ganze mehr ist als die Summe seiner Teile. Für die organisierte Informationsverarbeitung gilt daher, dass das Gesamtrisiko für die Grundrechte der Betroffenen größer ist als die Summe der Risiken, die in den einzelnen Phasen liegen.

Das Gutachten ist die erste Arbeit, in der fundiert über den zu verwendenden Informationsbegriff und dessen Angemessenheit zur Analyse und Lösung des Datenschutzproblems reflektiert wurde. Der Informationsbegriff, den die Autorinnen der Datenschutzanalyse und dem Datenschutzrecht zugrunde legen wollen, entstammt der Semiotik und besitzt vier Dimensionen: Syntax, Semantik, Pragmatik und Sigmatik.[309] Mit Syntax wird dabei die konkrete, meist zeichenmäßige Repräsentation bezeichnet. Mit Semantik wird die Bedeutung bezeichnet und mithin der Kontext adressierbar. Die pragmatische Dimension verweist auf den Zweck, dem die Information dienen soll, und die sigmatische Dimension bezeichnet die Relation zwischen Information und dem durch sie beschriebenen Objekt, im Bereich des Datenschutzes also die betroffene(n) Person(en), Gruppe(n), Organisation(en) oder Institution(en). Technische Systeme verarbeiten ausschließlich die syntaktischen Dimensionen von Informationen – technisch: Daten –, auch wenn die Informatik inzwischen langjährige Erfahrung darin hat, die anderen Dimensionen datentechnisch, d. h. syntaktisch, unter Verwendung von Meta-Daten zu simulieren.[310] Mit der Verwendung dieses Begriffs stellen die Autorinnen nicht nur sicher, dass Informationen in ihrer ganzen sozialen Komplexität rechtlich regulierbar sind,[311] sondern sie erzeugen auch kommunikative Anschlussfähigkeit für die moderne Soziologie, die Verwaltungswissenschaft und wenig überraschend auch für die Informatik. Der Begriff „Datenschutz“ soll aber gleichwohl beibehalten werden, da er „bereits eingebürgert“ sei.[312] Daraus ergibt sich klar und deutlich, dass die bis heute verwendeten Begriffe „personenbezogenes Datum“ und „personenbezogene Daten“ Informationsbegriffe sind.[313]

[307] Siehe die Ausführungen in Steinmüller et al. (1971, S. 57) zur grundlegenden Bedeutung der einzelnen Phasen: „in ihnen werden die Individualinformationen verarbeitet mit je spezifischen Auswirkungen und Gefährdungen für den Betroffenen.“

[308] Soziale Systeme sind grundsätzlich immer komplexe Systeme. Das gilt natürlich vor allem für Organisationen in modernen, differenzierten Gesellschaften.

[309] Siehe Steinmüller et al. (1971, S. 42 f.).

[310] Siehe ausführlich zum Informationsbegriff und seinen Folgen für das Datenschutzrecht Pohle (2014b). Zu den engen Grenzen eines algorithmischen Verstehens von Texten, d. h Zeichenketten, mit Computern siehe grundlegend Winograd und Flores (1986).

[311] Diese unterschiedlichen Dimensionen sind alle in der vorhergehenden *privacy*- und Datenschutzdebatte bereits an verschiedenen Stellen problematisiert worden, allerdings hatte bis dahin keine Diskussionsteilnehmerin die Konsequenz gezogen, einen geeigneten übergreifenden Informationsbegriff vorzuschlagen. Selbst die Notwendigkeit für einen solchen übergreifenden Begriff war bis zu diesem Zeitpunkt nicht formuliert worden.

[312] Steinmüller et al. (1971, S. 44, Fn. 8).

[313] Dabei gehen die Autorinnen wegen der „Umwandelbarkeit der Informationsarten“ davon aus, dass „die tatsächliche Vermutung für das Vorliegen einer Individualinformation“ spreche, siehe Steinmüller et al. (1971, S. 55 ff.), und verlangen daher, dass es dem Datenverarbeiter obliege, „diese Vermutung zu widerlegen.“ An anderer Stelle, in einem Vortrag, gehalten im Rahmen der Ringvorlesung „Anwendung der elektronischen Datenverarbeitung im Recht – Möglichkeiten und Probleme“ der Juristischen Fakultät der Universität München im Wintersemester 1971/72 und abgedruck in der Zeitschrift ÖVD 11/72, wird Steinmüller deutlicher: „Gegenstand des Datenschutzes sind also nicht die personenbezogenen Informationen, sondern *alle* Informationen, die in einem *konkreten* Informationssystem mit Hilfe von Zusatzinformationen und zugehöriger Programme im neuen Sinn verbunden werden können.“ Das ist – leider – keine Ablehnung des Begriffs der „personenbezo-

Die Autorinnen halten eine Konzeption des Datenschutzrechts ohne ein verfassungsrechtliches Fundament für keinen gangbaren Weg. Ihr Entwurf soll daher auf „zwei Säulen“ stehen: den Grundrechten und dem Rechtsstaatsprinzip.[314] Zwar betrachten die Autorinnen – jedenfalls kursorisch – auch die speziellen Grundrechte, soweit diese auch personenbezogene Informationen betreffen oder allgemein eine informationelle Dimension besitzen,[315] als den zentralen verfassungsrechtlichen Prüfungsmaßstab identifizieren sie jedoch die „freie Entfaltung der Persönlichkeit in Artikel 2 Absatz 1“ GG.[316] Auf der Basis einer – im Einzelnen durchaus kritikwürdigen – interdisziplinären Argumentation mit Anleihen aus der Kybernetik, der Soziologie und der Rechtswissenschaft versuchen sie zu zeigen, dass Art. 2 Abs. 1 GG „das Selbstbestimmungsrecht des Bürgers[317] über sein informationelles Personenmodell“ schützt.[318] Unterstützend – und nur unterstützend – wird zu dieser „Auslegung des Begriffs der Persönlichkeitsentfaltung“ auch die Menschenwürde als „übergeordnetes Verfassungsprinzip“ herangezogen, wonach der Mensch nicht zum „Objekt staatlichen Handelns“ gemacht werden dürfe.[319] Als zweite Säule des Datenschutzrechts betrachten die Autorinnen die „Grundprinzipien der staatlichen Ordnung“,[320] vor allem Gewaltenteilung und Rechtsstaatsprinzip. Damit begründen sie, warum erstens Zuständigkeitsgrenzen und zweitens die Grundsätze der Erforderlichkeit und der Gesetzmäßigkeit der Verwaltung – das Regelungsziel ist hier die Herstellung von (individueller und gesellschaftlicher, nicht informatischer) Berechenbarkeit von Grundrechtseingriffen – einzuhalten sind und es für Eingriffe in das Recht auf informationelle Selbstbestimmung einer gesetzlichen Ermächtigung bedarf.[321] Die Art und Weise der Bezugnahme auf diese Prinzipien ist allerdings aus zwei Gründen stark kritikwürdig. So werden erstens diese Prinzipien nur in ihren direkten Auswirkungen auf Art. 2 Abs. 1 GG betrachtet, nicht jedoch auch in ihrem Charakter als gesellschaftliche Instrumente zur Beschränkung struktureller Informationsmacht.[322] Zweitens wird zwar darauf verwiesen, dass die organisierte Informationsverarbeitung durch Private nicht den Rechtsstaatsanforderungen unterliege, die anschließend entwickelte Regelungsarchitektur wird jedoch unterschiedslos auf sowohl die öffentliche wie die private Informationsverarbeitung angewendet.[323]

genen Daten“, sondern dient ihrer genaueren Definition: „*Personenbezogene Daten sind systemrelativ.*“ Siehe Steinmüller (1972b), für die Zitate siehe S. 460, Hervorhebung im Original.

[314] Vergl. Steinmüller et al. (1971, S. 60).

[315] Einer der Beteiligten, Hansjürgen Garstka, wird später versuchen, das Datenschutzrecht tatsächlich als Schutz der informationellen Aspekte aller Grundrechte zu konzipieren, siehe Garstka (1977).

[316] Steinmüller et al. (1971, S. 85).

[317] Tatsächlich handelt es sich bei Art. 2 Abs. 1 GG nicht um ein exklusives Bürger- oder Deutschengrundrecht, sondern um ein Menschenrecht.

[318] Steinmüller et al. (1971, S. 88). Die Autorinnen entwickeln diese Begründung unter anderem unter Verweis auf Luhmann (1986) und Talcott Parsons. Parsons wird dabei nicht einmal selbst zitiert, sondern nur „nach König“, siehe Steinmüller et al. (1971, S. 87, Fn. 39). Für die Quellenangabe „Turner, 1032“ in Fn. 38 enthält das Literaturverzeichnis gleich gar keinen Eintrag.

[319] Steinmüller et al. (1971, S. 88). Seit dem Volkszählungsurteil wird – auch rückwirkend – angenommen, dass das Recht auf informationelle Selbstbestimmung eine Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sei, und dass das allgemeine Persönlichkeitsrecht damit auch die verfassungsrechtsliche – und mehr noch: (rechts-)architektonische – Grundlage des Datenschutzrechts darstelle. Eine solche Fehlannahme kann der Architektur des Datenschutzrechts – und mithin auch den ihm immanenten Beschränkungen – allerdings nicht gerecht werden.

[320] Steinmüller et al. (1971, S. 90).

[321] Vergl. Steinmüller et al. (1971, S. 90 ff.).

[322] Dabei hatten die Autorinnen das Problem der strukturellen Informationsmacht in ihrer allgemeinen Darstellung der Auswirkungen der Industrialisierung der gesellschaftlichen Informationsverarbeitung durchaus ausführlich angesprochen, wenn auch fast ausschließlich in Bezug auf die vertikale und horizontale Gewaltenteilung.

[323] Damit soll nicht behauptet werden, dass Private auf keinen Fall Rechtsstaatsanforderungen unterworfen werden könnten, siehe etwa den Vorschlag von Citron (2008), aber dann ist erhöhten Begründungserfordernissen zu ge-

Die vorgeschlagene Regelungsarchitektur spiegelt die identifizierte Phasenorientierung jeder organisierten Informationsverarbeitung wider.[324] Im Einzelnen analysieren die Autorinnen die Phasen „Informationsermittlung“[325] als „Beschaffung (Aufsuchen) und Auswahl von Informationen“, „Informationserfassung“[326] als „Transformation von Informationen in Daten“, „Informationsspeicherung“[327] als „Festhalten der erfaßten Information zur weiteren Verwendung“, „Informationsveränderung“[328] entweder als „inhaltliche Umgestaltung einer gespeicherten Information“, als „Verknüpfung von Informationen und [der] sich daraus ergebende[n] Gewinnung neuer Informationen“ oder als „Änderung der Benutzerzuordnung“[329], „Informationsweitergabe“[330] mit den Fallgruppen „Informationsveröffentlichung“, „Informationsaustausch“, „Informationsweitergabe an Dritte“ und „Informationsverbund“ sowie die „Informationslöschung“,[331] „so daß ihre Verwendung in keiner Weise mehr möglich ist.“ Für diese Phasen werden dabei jeweils die Interessen der Beteiligten und die möglichen Gefährdungen ermittelt und dann rechtliche Anforderungen an die Informationsverarbeiter formuliert. Anschließend werden zusammengefasst die Betroffenrechte erörtert: Unterrichtungsansprüche, das Auskunftsrecht, das Datenjournal[332] sowie als Folgeansprüche der Berichtigungsanspruch und der Löschungsanspruch.[333] Abschließend betrachten die Autorinnen die organisatorischen Kontrollmöglichkeiten.[334]

Ruprecht Kamlahs Arbeit „Datenschutz im Spiegel der anglo-amerikanischen Literatur“[335] stellt eine Aktualisierung und Erweiterung der Ausführungen in seiner 1969 veröffentlichten Dissertation „Right of Privacy“[336] dar, wenn auch in sehr viel kürzerer Form. Die von Kamlah für den englischsprachigen Diskurs als die wichtigsten Arbeiten identifizierten sind dabei jene von Arthur R. Miller, Alan F. Westin sowie Malcolm Warner und Michael Stone.[337] Laut Kamlah könne von einer Tendenz gesprochen werden, die dahin geht, „die Verwendung personenbezo-

nügen. Die von den Autorinnen präsentierten Begründungen, siehe S. 137 ff., genügen den Anforderungen jedoch nicht, insbesondere wenn sie behaupten, dass auch private „Informationssysteme als soziale Gewalten grundsätzlich keine Grundrechte gegenüber dem Bürger geltend machen können“ Steinmüller et al. (1971, S. 140). Eine Kritik daran, dass strukturell mächtige soziale Akteurinnen Grundrechte gegenüber weniger mächtigen geltend machen können, ist vor dem Hintergrund, dass Grundrechte zur Konditionierung von Machtverhältnissen zugunsten der weniger mächtigen Akteurinnen entwickelt, ausgehandelt und erkämpft wurden, jedoch notwendig.

[324] Siehe Steinmüller et al. (1971, S. 57 ff.). Auch hier folgen die Autorinnen in allen Fällen der bereits bestehenden Benennung der einzelnen Phasen, obwohl sie selbst zugeben, dass das nicht unproblematisch sei, siehe S. 57.

[325] Vergl. Steinmüller et al. (1971, S. 93 ff.).

[326] Vergl. Steinmüller et al. (1971, S. 104 f.).

[327] Vergl. Steinmüller et al. (1971, S. 105 f.).

[328] Vergl. Steinmüller et al. (1971, S. 106 ff.).

[329] Damit ist gemeint, dass ein Benutzerwechsel stattfindet, wobei mit Benutzern von Informationen Datenverarbeiter bezeichnet werden.

[330] Vergl. Steinmüller et al. (1971, S. 110 ff.).

[331] Vergl. Steinmüller et al. (1971, S. 123).

[332] „[D]ie Auskunft ist bei EDVA [Elektronischen Datenverarbeitungsanlagen] ohne Datenjournal nicht ausreichend zu erteilen.“ Steinmüller et al. (1971, S. 125). Den von den Autorinnen geforderten „Datensichtstationen“ entsprechen beim heutigen Stand der Technik direkte Online-Abfragemöglichkeiten für die Betroffenen.

[333] Vergl. Steinmüller et al. (1971, S. 123 ff.).

[334] Vergl. Steinmüller et al. (1971, S. 126 ff.). Wie auch Podlech fordern sie eine Veröffentlichungspflicht für Computerprogramme, die zur Verarbeitung personenbezogener Daten dienen, siehe S. 129.

[335] Kamlah (1971a).

[336] Siehe Kamlah (1969).

[337] Miller (1969), Westin (1966a), Westin (1966b), Westin (1967) und Warner und Stone (1970), siehe Kamlah (1971a, S. 197, Fn. 4). Für einen umfassenden Überblick über die englischsprachige, vor allem die amerikanische Debatte, siehe auch die Darstellung unter 2.3.1, S. 18 ff.

gener Daten weiter zu verrechtlichen.“[338] Er meint, drei Bereiche identifizieren zu können, mit denen sich die Diskussion beschäftige: die Frage nach den Rechtsgrundlagen für das Sammeln und Speichern von personenbezogenen Daten, die Frage nach den Rechtsgrundlagen für deren Weitergabe sowie die Frage nach einer Pflicht, Daten periodisch zu löschen. Anschließend betrachtet Kamlah die technischen Schutzmaßnahmen, die „so gut wie alle Autoren“ verlangen, jedoch nur wenige tatsächlich beschreiben würden.[339] Kamlahs dritter Abschnitt gibt einen Überblick über die Aufsichtsorganisation, von der Frage einer Anzeige- oder Erlaubnispflicht über den Anknüpfungspunkt für gesetzliche Regelungen bis hin zum Aufsichtsgremium.[340] Im vierten und letzten Abschnitt reflektiert Kamlah die amerikanische Diskussion über die Betroffenenrechte, unter die er allerdings auch die Frage nach einer Protokollierungspflicht für Datenverarbeiter fasst.[341] Kamlah schließt mit der Wiedergabe der Beteuerung von „Computerexperten“, „daß sie viel tun können, wenn ihnen nur endlich gesagt wird, was, wie und vor wem zu schützen ist.“[342]

Die von Karl Steinbuch und Herbert Wacker angestellten „Überlegungen zu technischen Möglichkeiten des Datenschutzes im Hinblick auf ein Bundesdatenschutzgesetz“[343] stellen nicht gerade einen Meilenstein in der Debatte dar. Steinbuch und Wacker gehen wie so viele Technikerinnen davon aus, unter „Datenschutz“ verstehe frau „zunächst den Schutz gegen unberechtigten Zugriff, er umfaßt auch alle Maßnahmen zum Schutz der Daten gegen Verfälschung, Mißbrauch oder Zerstörung durch Unbefugte“, gefolgt von „Der Datenschutz ist zunächst ein rechtliches Problem: Es muß geklärt werden, wer, wann, wo, was eingeben, abfragen, ändern oder löschen darf.“[344] Anschließend folgen die zeittypischen Darstellungen von Benutzererkennung und Überprüfung der Zugriffsberechtigung. Die Autoren stellen danach „die Frage, nach welchen Kriterien man Verfahren des Datenschutzes beurteilen kann“ und beantworten sie unter Verweis auf die Kriterien der Schutzwürdigkeit der Daten („Dahinter verbirgt sich die Frage, welchen Schaden ein Mißbrauch zur Folge haben könnte.“), der Sicherheit gegen unerlaubte Zugriffe durch Unbefugte, der Adaptionsmöglichkeit und Flexibilität des Sicherheitssystems, des Aufwands und der Kosten sowie der Benutzerfreundlichkeit.[345] Die Forderungen nach technisch-organisatorischen Schutzmaßnahmen umfassen die nach einem „closed-shop-Betrieb“, nach der Unmöglichmachung, bestimmte Funktionen von „anschaltbaren Datenstationen“ aus, also vernetzten Rechnern, auslösen zu können, nach vollständiger Protokollierung aller das Schutzsystem betreffenden Tätigkeiten, nach vorheriger – und danach regelmäßig wiederholter – Austestung der Schutzvorkehrungen sowie nach der Einsetzung einer IT-Sicherheitsbeauftragten.[346] Eine Protokollierung aller Verarbeitungen personenbezogener Daten und ein darauf aufbauendes Auskunftsrecht der Betroffenen lehnen Steinbuch und Wacker aus Gründen des „ungeheuere[n] Aufwand[s]“ ab. Statt dessen solle sich das Auskunftsrecht „in der Regel auf den aktuellen Bestand“ an Daten beschränken.[347]

[338] Siehe Kamlah (1971a, S. 199 ff.).
[339] Kamlah (1971a, S. 202). Es handelt sich hier mit einer Ausnahme durchgehend um Maßnahmen aus dem Bereich der IT-Sicherheit. Die Ausnahme besteht in der Frage der „Festsetzung von Geheimhaltungsstufen“ (S. 203), wie sie etwa von Arthur Miller – oder auch, aber von Kamlah nicht zitiert, von Jon Bing – gefordert werden. Kamlah selbst hält eine solche Einstufbarkeit für ausgeschlossen, siehe Kamlah (1970, S. 364).
[340] Kamlah (1971a, S. 204 ff.). Als Anknüpfungspunkt identifiziert Kamlah „Datenbanken“, unter denen etwa der Computer als formelles oder die Datensammlung als materielles Kriterium verstanden werde (a. a. O.).
[341] Kamlah (1971a, S. 206 ff.).
[342] Kamlah (1971a, S. 211).
[343] Steinbuch und Wacker (1972).
[344] Steinbuch und Wacker (1972, S. 216).
[345] Siehe Steinbuch und Wacker (1972, S. 217).
[346] Siehe Steinbuch und Wacker (1972, S. 219 f.).
[347] Siehe Steinbuch und Wacker (1972, S. 220 ff.).

2.3.4 Die kurze Phase der Interdisziplinarität

Der Zeitraum zwischen 1972 und 1978 kann unzweifelhaft als Hochzeit der interdisziplinären Auseinandersetzung über Fragen des Datenschutzes bezeichnet werden. Dieser Zeitraum ist geprägt von einer Reihe von Veranstaltungen, auf denen Vertreterinnen verschiedener wissenschaftlicher Disziplinen miteinander, aber auch mit einer politisierten Öffentlichkeit versuchten, den Datenschutz in seiner ganzen thematischen Breite und seinen Voraussetzungen und Folgen fundiert zu beleuchten.[348] Bemerkenswert ist dabei auch der Umstand, dass viele Fachvertreterinnen Versuche unternahmen, die eigenen Fachgrenzen zu überschreiten und sich das theoretische und methodologische Handwerkszeug anderer Disziplinen nutzbar zu machen.

Auf Einladung der Deutschen Forschungsgemeinschaft fand vom 02.–04.11.1972 in Regensburg eine Tagung zu den „sozialen, politischen und rechtlichen Konsequenzen der Einführung moderner Informationstechnologien in Management und Verwaltung“ statt. Während nach den Veranstalterinnen die Schwerpunkte der Diskussion in den Vorjahren „auf den Fragen der Gefährdung der Privatsphäre und der Verschiebung des Informationsgleichgewichts zwischen Regierung und Parlament“ gelegen habe, ginge es nun um grundsätzlichere Fragen, nämlich „um die Stellung des Individuums insgesamt.“[349]

Podlech will in seinem Beitrag eine Begründung für seinen Entwurf zu einem „Bundes-Datenschutz-Rahmengesetz“ vom Juli 1972 liefern.[350] Im ersten Teil der Arbeit gibt Podlech den Stand der Gesetzgebung auf dem Gebiet des Datenschutzes wieder, während er im zweiten Teil die zentralen Kennzeichen der bisherigen Datenschutzgesetze darstellt. Alle Entwürfe gingen aus „von der Privatsphäre des Einzelnen.“ Sie versuchten zu verhindern, dass „Informationen aus dieser Privatsphäre unberechtigt verwendet werden.“ Weder werde die Privatsphäre näher umschrieben noch finde eine Auseinandersetzung mit diesem in der Literatur kritisierten Begriff statt. Alle Entwürfe würden den Bürgerinnen Auskunfts-, Unterlassungs- und Schadensersatzansprüche gewähren und Geheimnisverletzungen (als Teil des Nebenstrafrechts) mit Strafen und Geldbußen belegen. Alle Entwürfe – bis auf den des Bundesministeriums des Innern[351] – sähen eine Aufsichtsbehörde mit Kontroll- und Aufsichtsrechten vor.[352] Im dritten Teil beschreibt Podlech die Ausgangslage für seinen Entwurf, aus der er im vierten Teil Folgerungen für die von ihm formulierten Regelungen zieht.[353] Ausgangslage ist die Planung des Bundes und aller Bundesländer für die Einführung integrierter Informationssysteme, deren Grundlage ein bundeseinheitliches Personenkennzeichen sein solle.[354] Wenn integrierte Informationssysteme erst einmal eingerichtet seien, dann ließe sich ihre Struktur nicht mehr grundlegend ändern. Da-

[348] Das geschah, wie Paul J. Müller später einräumte, durchaus nicht immer ganz uneigennützig, siehe Rost (2012a), ab Minute 31:30. Das Institut für angewandte Sozialforschung der Universität zu Köln, an dem Müller arbeitete und forschte, gehörte zu den ersten großen Nutzern von Computern für die wissenschaftliche Auswertung umfangreicher empirischer Untersuchungen. In dem Maße, wie die Beteiligten eine wissenschaftlich fundierte soziologische Analyse des Datenschutzproblems vorlegten, konnten sie zumindest verhindern, dass die Wissenschaft in ihrer Gesamtheit, die an vielen Stellen durchaus große Mengen personenbezogener Daten erhebt und verarbeitet, auch noch die negativen Folgen einer falschen Problemanalyse würde tragen müssen.

[349] Kilian et al. (1973, S. V).

[350] Siehe Podlech (1973b, S. 3). Er kündigte gleichzeitig die Veröffentlichung einer geänderten und erweiterten Fassung seiner Begründung zusammen mit seinem Gesetzentwurf in einem Beiheft der Zeitschrift DVR an, siehe Podlech (1973a).

[351] Spätere Gesetzentwürfe aus dem BMI enthalten dann ebenso wie das BDSG 1977 eine solche Aufsichtsbehörde.

[352] Podlech (1973b, S. 5 f.).

[353] Podlech (1973b, S. 6 ff.).

[354] Dieses Kennzeichen wurde dann nach langer Diskussion 1976 sehr dauerhaft aufs Abstellgleis geschoben, weil parteiübergreifend Einigung über dessen Verfassungswidrigkeit bestand. Inzwischen gibt es ein Äquivalent zum PKZ: die Steueridentifikationsnummer. Schon damals war in der Datenschutzdebatte breit akzeptiert, dass es

tenschutz müsse aber gerade bei der grundlegenden Struktur ansetzen, verlangt Podlech. Der wichtigste Schutzmechanismus bestehe in der organisatorischen Maßnahme der Trennung zwischen Betreiberin und Nutzerin der Datenverarbeitung, gefolgt vom „Programmschutz“, der Zertifizierung der eingesetzten Technik und der Programme durch eine unabhängige Instanz. Erst auf dieser Basis ließen sich sinnvoll Rechte der Betroffenen und Strafbestimmungen formulieren und durchsetzen.[355] Podlech verweist darauf, dass ohne regelmäßige Kontrollen durch externe Stellen kein datenschutzkonformes Verhalten der datenverarbeitenden Stellen garantiert werden könne. Es gebe eine „Vermutung regelwidrigen Verhaltens unkontrollierter sozialer Systeme.“[356] Im fünften und letzten Teil seiner Arbeit setzt Podlech den Datenschutz im Bereich der öffentlichen Verwaltung in den größeren Kontext eines umfassenden Informationsrechts, das den Datenschutz sowohl im Bereich der öffentlichen Verwaltung wie im Bereich der Wirtschaft regele und ergänzt werde durch ein Recht auf Informationsfreiheit, „den korrespondierenden Gesichtspunkt des freien Zugangs zu gesellschaftlich relevanten Informationen.“[357]

Klaus Lenk konzentriert sich in seiner Arbeit auf die Veränderungen im Verhältnis zwischen Staat und Individuum, die er als Folgen der zunehmenden Automatisierung der Informationsverarbeitung durch die staatliche Verwaltung sieht.[358] Vor dem Hintergrund der Verwaltungsrationalisierung, die die Gefahr negativer Konsequenzen für das Verhältnis Bürgerin–Verwaltung heraufbeschwöre, erscheine der Datenschutz in der Diskussion als ein Mittel, diesen negativen Auswirkungen zu begegnen. Letztendlich heiße das nichts anderes, als dass gerade die Befürworterinnen eines starken Datenschutzes diesen fordern, um damit die Ausweitung der automatischen Datenverarbeitung individuell und gesellschaftlich erträglich und damit durchsetzbar zu machen.[359] Durch die „funktionelle Zentralisierung“ der Informationsspeicherung und -verarbeitung werde das Individuum für alle Bereiche der Verwaltung gleich sichtbar. Mit dem dabei eintretenden Verlust an „administrativer Gewaltenteilung“ erhöhe sich die Gefahr einer „sachwidrigen Kopplung“ mehrerer Verwaltungstätigkeiten, wodurch „die Leistung einer Stelle von politischem Wohlverhalten gegenüber der anderen Stelle abhängig gemacht“ werde oder zumindest werden könne. Insbesondere bestehe auch die Gefahr, dass Leistungs- und Planungsdaten für Überwachungszwecke eingesetzt würden, wobei allein „das Vorhandensein des größeren Überwachungspotentials“ zu derartigen Forderungen führen werde – womit Lenk die Gegenwart sehr genau vorherbeschrieben hat. Und nicht zuletzt könne die zunehmende Integration von (auch anonymisierten) Daten aus verschiedenen Quellen zu einer stärkeren Durchleuchtung individueller und gesellschaftlicher Gewohnheiten und Vorgänge führen und mithin zu einer verbesserten staatlichen Steuerbarkeit gesellschaftlicher Verhältnisse. Diese Durchleuchtung lasse sich, so Lenk, „als Bedrohung der Privatsphäre nicht mehr fassen.“[360] Zwar will Lenk, dass technische und organisatorische Schutzmaßnahmen sofort umgesetzt werden sollen, allerdings will er gleichwohl eine „exaktere Bestimmung der möglichen Gefahren anregen.“ Die Grundfrage des Datenschutzes sei, „wieviel personenbezogene Daten die einzelnen staatlichen Teilbürokratien brauchen, um ihre Aufgaben zu erfüllen.“ Dazu müssten die einzelnen Aufgaben klarer definiert werden, um daraus auf den Informationsbedarf schließen zu können. Lenk fordert eine Unter-

keiner expliziten PKZ bedarf, um deren Integrationsfunktion zu erfüllen, siehe Rost und Krasemann (2008), ab Minute 18:58.

[355] Podlech (1973b, S. 7 f.).

[356] Podlech (1973b, S. 10 f.).

[357] Podlech (1973b, S. 11).

[358] Lenk (1973).

[359] Siehe Lenk (1973, S. 15, 18).

[360] Siehe Lenk (1973, S. 21 ff.).

suchung der Datenelemente daraufhin, „wie stark sie die betroffenen Personen berühren." Dies hänge allerdings „nicht von irgendwelchen natürlichen Eigenschaften dieser Daten" ab, sondern von deren Verwendungszweck und -zusammenhang.[361] Eine der Aufgabe von Kontrollinstitutionen sei nach Lenk die Durchsetzung der Akzeptanz von Kosten technischer Datenschutz- und Datensicherheitsmaßnahmen als notwendige Kosten.[362]

Steinmüller präsentiert in seinem Beitrag wieder seine systemtheoretisch begründete Datenschutzkonzeption.[363] Er beschreibt den Individualdatenschutz – als Gegenstück zum Institutionaldatenschutz – nicht nur als Schutz des Individuums, sondern auch – weil moderne Demokratie auch Minderheitenschutz sei – als Schutz von Gruppen[364] vor einem aus fünf Elementen bestehenden Informationssystem: 1. Hardware, 2. Software, 3. Daten, 4. Organisation, 5. System-Umwelt-Kopplung.[365] Steinmüller meint, aus der Variabilität und Adaptivität der Systeme schließen zu können, das alles gar nicht so schlimm sei: Wer vor dem Hintergrund der „Anpassungsfähigkeit der Rechner und ihrer Strukturen" die Existenz technischer Sachzwänge behaupte, verberge hinter diesem Argument entweder wirtschaftliche oder politische Ziele oder eigenen technischen Unverstand.[366] Er hingegen versuche, alle drei Ziele des von ihm identifizierten „magischen Dreiecks" zu erfüllen: Funktionsfähigkeit der Verwaltung, EDV-gerechte Organisation der Verwaltungautomation, Schutz der Bürgerinnen sowie der Gruppen und Institutionen der Gesellschaft.[367]

Hans Brinckmann versucht in seinem Beitrag, das Verhältnis zwischen Datenschutz und Informationsfreiheit zu bestimmen.[368] Beide stünden in einem grundsätzlichen Spannungsverhältnis zueinander.[369]

Bernt Bühnemann behauptet in seinem Beitrag,[370] dass die „Gefahren des Mißbrauchs" im privatwirtschaftlichen Bereich größer seien als im öffentlichen Bereich, da staatliche Tätigkeit im Verhältnis zu den Bürgerinnen erstens dem Gesetzesvorbehalt unterliege und zweitens insbesondere durch den Status negativus der Staatsbürgerin gebremst werde, während dem privatwirtschaftlichen Handeln wesentlich geringere Limitierungen auferlegt seien.[371] Eine generalisierende Regelung des Datenschutzes im privatwirtschaftlichen Bereich scheide allerdings aus. Statt dessen müssten die Regelungen in Beziehung gesetzt werden zu Art und Zwecken der Datenverarbeitung. Bühnemann will insbesondere nach Wirtschaftsbereichen trennen. Dafür sollen drei Prämissen gelten: „1. Die Privatwirtschaft ist ohne ein Mindestmaß an Informationen

[361] Siehe Lenk (1973, S. 34 ff.).
[362] Siehe Lenk (1973, S. 47).
[363] Steinmüller (1973).
[364] Steinmüller (1973, S. 53).
[365] Steinmüller (1973, S. 54 f.). Hardware, Software und Daten bilden dabei ein Datenverarbeitungssystem, das in eine „funktionelle und institutionelle Organisation" eingebettet sei. „Dadurch erst entsteht das Mensch-Maschine-Kommunkationssystem, kurz auch »Mensch-Maschine-System«." Das System sei nicht isoliert, sondern eingebettet in ein umgebendes System, das „Umsystem". Mit diesem finde ein Austausch von Daten, Programmen und Menschen statt. Das Umsystem gebe dem System Ziele vor. Siehe Steinmüller (1973, S. 55).
[366] Steinmüller (1973, S. 59).
[367] Steinmüller (1973, S. 66).
[368] Brinckmann (1973).
[369] Brinckmann (1973, S. 77 f.). Diese Aussage trifft er allerdings unter Verkennung der sozialen Machtbeziehung zwischen den unterschiedlichen Akteurinnen. Datenschutz kann danach als Abwehrrecht der Schwächeren im Informationsmachtverhältnis beschrieben werden. Die gleiche Akteurin wird aber auch von der Informationsfreiheit bevorteilt: mit einem Recht auf Informationszugang. Die konzeptionellen Gegenstücke bevorteilen jeweils die Stärkere im Informationsmachtverhältnis: Verdatungsfreiheit und die von Brinckmann selbst problematisierte „überkommene Arkanpraxis", siehe Brinckmann (1973, S. 81).
[370] Bühnemann (1973).
[371] Bühnemann (1973, S. 98 f.).

funktionsunfähig. 2. Die Datenverarbeitung wird in der Privatwirtschaft vornehmlich für wirtschaftliche Zwecke eingesetzt. 3. Der Schutz des Individuums muß grundsätzlich Vorrang haben vor dem Schutz des Privatwirtschaftsverkehrs.“[372] Bühnemann verlangt, sich bei der Regelung des Datenschutzes an bereits erfolgreich umgesetzten Maßnahmen zu orientieren und etwa auf Erfahrungen aus dem Versicherungsrecht oder dem Bankenaufsichtsrecht zurückzugreifen und diese zu erweitern.[373]

Andrea Hasselkuss und Claus-Jürgen Kaminski versuchen in ihrem Beitrag, Hubmanns Sphärentheorie wieder zur Grundlage der Datenschutzdiskussion zu machen und sich gleichzeitig von der amerikanischen *privacy*-Debatte abzugrenzen.[374] Auch wenn sie keine neuen Aspekte zur Sphärentheorie beitragen, ziehen sie am Ende den Schluss, dass die Diskussion über deren Verwendbarkeit weitergeführt werden sollte, solange es nicht gelinge, ein alternatives System für den Datenschutz zu entwickeln, das deren Mängel nicht aufweise.[375]

Bernhard Schlink analysiert, welche Folgen es habe, dass die Verwaltung die Bürgerin zum „Datenobjekt“ mache.[376] Zu Beginn versucht er zu ermitteln, ob es ein verfassungsmäßiges Recht auf Selbstdarstellung für das Individuum gebe. Das lehnt er ab:

> „Ein Recht des Bürgers zur Selbstdarstellung gegenüber der Verwaltung wäre also damit erkauft, daß der Bürger zu Recht der Verwaltung als Person ausgesetzt ist, und ginge auf Kosten des Persönlichkeitsschutzes, den gerade das rechtsstaatliche unpersönliche Verhältnis zwischen Bürger und Verwaltung bietet. Aus diesem, nicht aus einem Selbstdarstellungsrecht des Bürgers ist das Verbot der Erstellung und Verwertung umfassender Persönlichkeitsbilder abzuleiten.“[377]

Eine der Gefahren einer solchen Vollerfassung sei die Möglichkeit der „sachwidrigen Koppelung von Verwaltungsobliegenheiten“, wenn also eine Behörde ihr Handeln gegenüber einer Bürgerin von deren Verhalten gegenüber einer anderen Stelle oder Person abhängig mache (Koppelung), und diese Koppelung gesetzlich nicht vorgesehen sei.[378] Schlink fordert, dass die Bürgerin Auskunft stets dann verweigern könne, „wenn mit einer Verwendung und insbesondere einer Weitergabe der Auskunft durch die ermittelnde Verwaltungsbehörde zu rechnen ist, die durch Gesetz, Amtshilfepflicht und Hoheitsfunktion der Behörde nicht gedeckt ist.“ Der Schutz reiche aber nicht aus, wenn der Behörde die Daten bereits vorliegen. Die Bürgerin müsse dann „auf

[372] Bühnemann (1973, S. 101).

[373] Bühnemann (1973, S. 102 f.).

[374] Hasselkuss und Kaminski (1973). Insbesondere verlangen sie die Einstellung der Versuche, das Rechtsinstitut der „privacy“ mit der „Privatsphäre“ gleichzusetzen, siehe S. 109: „Als »right of privacy« wurde im amerikanischen Recht, basierend auf einem grundlegenden Aufsatz von Warren und Brandeis, ein Rechtsinstitut entwickelt, das dem einzelnen einen Schutz vor Indiskretionen, falscher Berichterstattung und ähnlichen Eingriffen in seinen persönlichen Bereich gab. Dieser Begriff wird im Deutschen oft mit »Privatsphäre« gleichgesetzt. Die Übersetzung ist zweifach bedenklich. Der Begriff »Privatsphäre« ist ein juristischer Begriff im deutschen Rechtskreis, und es scheint aus rechtsvergleichender Sicht bedenklich, zwei Rechtsinstitute in verschiedenen Rechtskreisen ohne Bezug auf das System einfach gleichzusetzen. Zudem ist gerade der persönlichkeitsrechtliche Bereich in jeder Rechtsordnung anders entwickelt und geradezu ein Charakteristikum für sie.“

[375] Siehe Hasselkuss und Kaminski (1973, S. 128).

[376] Schlink (1973).

[377] Schlink (1973, S. 159). Dieser Gedanke ist bislang an keiner Stelle wieder aufgegriffen worden, obwohl er bei der Begründung des Profilbildungsverbots ohne die so oft vorgebrachten Befindlichkeiten des Individuums auskommt.

[378] Siehe Schlink (1973, S. 159). Das Verbot sachwidriger Koppelung habe Forsthoff auf den Begriff der „Trennung der Gewalten innerhalb der Verwaltung“ gebracht. Das entspricht dem heute gebräuchlichen Begriff der „informationellen Gewaltenteilung“.

den vorhandenen Datenbestand selbst“ Einfluss nehmen können.[379] Er hält daher ein Recht auf Löschung, Korrektur oder Ergänzung vorhandener Daten für notwendig und verweist auf das Bundesverwaltungsgericht, welches das institutionalisierte Vergessen aus dem Menschenbild des Grundgesetzes begründet habe. Schlink zufolge handele es sich dabei um einen „Folgenvorbeugungsanspruch“, der „auf den Rechtsschutz des Bürgers als Datenobjekt gerade zugeschnitten“ sei.[380]

Hansjörg Geiger verlangt in seinem Beitrag[381] nach dem Vorbild von Podlech, Simitis, Steinmüller und Schneider eine Ausweitung des Schutzgutes des Datenschutzes auf „die Gesellschaft als Ganzes, Teile von ihr bzw. den einzelnen Bürger sowie den Informationshaushalt.“[382] Er schlägt einen parlamentarischen Datenschutz-Ausschuss vor – ähnlich dem Verteidigungsausschuss –, der sowohl die Rolle der modernen Datenschutzbeauftragten (inklusive ihrer Rechte und Pflichten, weshalb ihnen auch nicht der Datenschutz als Argument für staatliche/behördliche Arkanpolitik vorgehalten werden könne), die eines institutionellen Informationsgegengewichts zur Exekutive als auch die eines „globalen Ausbalancierers“ im Informationsverhältnis zwischen allen drei Gewalten spielen solle.[383]

Während Geiger das Problem der Gewaltenteilung aus einer „mehr staatsrechtlich-politikwissenschaftliche[n] Sicht“ betrachte, analysiert Lutterbeck dessen „entscheidungstheoretische Komponente“.[384] Er schlussfolgert, dass die Datenschutzdiskussion nicht nur um Fragen des Informationsgleichgewichts, sondern auch um den Aspekt der Planungskontrolle erweitert werden müsse, weil diese sachlich zusammengehörten.[385]

In seinem Beitrag versucht sich Garstka an einer Definition und Abgrenzung der im Datenschutzbereich verwendeten Begriffe, präsentiert dabei aber nichts Neues.[386]

Jochen Schneider diskutiert in seinem Beitrag die technischen Möglichkeiten des Datenschutzes, worunter er „alle die Maßnahmen [. . .] verstehen [will], die als Realisierung der Anforderungen des Datenschutzes eingesetzt werden.“[387] Dabei weist er darauf hin, dass die konventionellen Datenverarbeitungsmaßnahmen „keineswegs“ so sicher seien, wie es von der EDV erwartet werde. Die entscheidenden Unterschiede liegen nach Schneider in „Informations-Potential, Wiederholbarkeit und Problematik der Feststellung.“ Diese Unterschiede würden die „wesentlich höheren Anforderungen“ rechtfertigen.[388] Schneider ist einer der Wenigen, die technisch argumentieren, jedoch nicht auf die falsche Selbstbeschränkung des Verhinderns von etwas „Unbefugten“ hereinfallen: „Missbrauch“ könne zwar der unberechtigte Umgang mit Daten sein, jedoch auch der „legitime bzw. legitimierte.“[389] An der „Relativität der Privatsphäre“ würde eine „Klassifizierung von Daten“ scheitern, so Schneider, und mehr noch: Es fehle „die Möglichkeit genereller Festlegung von Empfindlichkeit, Schutzbereich oder Persönlichkeitswert.“[390]

[379] Siehe Schlink (1973, S. 164 f.).
[380] Siehe Schlink (1973, S. 165 ff.).
[381] Geiger (1973).
[382] Geiger (1973, S. 174).
[383] Geiger (1973, S. 182 ff.). Von allen Landesdatenschutzbeauftragten hat nur die hessische die Aufgabe, die Informationsmachtbalance zwischen den Gewalten zu beobachten, damals in § 10 Abs. 2 HDSG, heute in § 24 Abs. 2 HDSG.
[384] Lutterbeck (1973, S. 188).
[385] Siehe Lutterbeck (1973, S. 198).
[386] Garstka (1973).
[387] Schneider (1973, S. 224).
[388] Schneider (1973, S. 224, Fn. 12).
[389] Schneider (1973, S. 224).
[390] Schneider (1973, S. 229). Der Rest seiner Arbeit besteht aus der Aufzählung einzelner Verfahren wie Authentifizierung oder Protokollierung auf dem damaligen Stand der Technik.

Ulrich Dammann analysiert in seinem Beitrag das Hessische Planungsinformations- und Analyse-System (HEPAS), das zum Zeitpunkt des Erscheinens gerade im Entstehen begriffen war.[391] HEPAS bestehe aus der sogenannten Datenbasis und der sogenannten Methodenbasis („Programme, mit denen aus diesen Daten Entscheidungshilfe gewonnen werden sollen"). Die Datenbasis solle aus den „im automatischen *Verwaltungsvollzug* entstehenden Daten" sowie Daten aus der amtlichen Statistik gespeist werden. Hinzu kämen Daten aus sonstigen Statistiken, Erhebungen und Umfragen. Es gebe ein geographisches Identifizierungsmerkmal (GID), das Planquadraten (1000 m Seitenlänge, bzw. 200 m in besiedelten Gebieten) zugeordnet sei und als Ordnungskriterium dienen soll.[392] Dammann weist darauf hin, dass die Nutzung statistischer Daten allein nicht bedeutet, diese seien nicht individualisierbar. Die falsche Ansicht speise sich wohl aus der Beobachtung, dass Veröffentlichungen statistischer Ämter „in der Tat keine Einzelangaben enthalten dürfen." „Aggregiert und anonymisiert" seien jedoch nur die veröffentlichten Ergebnisse, in den meisten Fällen nicht aber die gespeicherten Daten. Weiterhin zeigt Dammann, dass insbesondere Systeme für Planungs- und Entscheidungshilfen immer individualisierende Daten speichern müssten, weil sie zumindest in der Lage sein müssten, Informationen, die dasselbe Objekt betreffen, miteinander zu verknüpfen.[393]

Dieter Rave betrachtet in seinem Beitrag die Datenschutzprobleme, die es im Gesundheitswesen gebe.[394] Er sieht das Gesundheitswesen als gutes Beispiel dafür, „daß die Datenschutzdiskussion ins falsche Geleis [sic] gerät, wenn sie sich in die liberale Ecke »Schutz- und Abwehrrechte der vereinzelten Individuen gegenüber dem übermächtigen Staat« abdrängen" lasse, das die Ausweitung der Staatsfunktionen einen „vom Staat abgrenzbaren Privatbereich tendenziell verschwinden" lasse. Eine angemessene Regelung müsse stattdessen auf ein „Datenverkehrsrecht" hinauslaufen.[395] Aufgabe von Datenschutzregelungen sei es, „die Verfügungsgewalt über Informationen zu regeln."[396] Rave kritisiert insbesondere die auch heute noch weitverbreitete Bezugnahme auf ein angeblich existierendes Geheimhaltungsinteresse:

> „Das Interesse der Betroffenen an Geheimhaltung, mit dem so oft operiert wird, ist solange kein ausreichendes Kriterium für die Ausgestaltung des Datenschutzes, wie:
>
> - im Gesundheitswesen die ungebrochene Autoritätskultur fortbesteht, der Patient also unwidersprochen fast alles mit sich geschehen läßt,
> - die Staatsbürger alle angeforderten Informationen preiszugeben bereit sind, wenn sie im Ausgleich dafür Leistungen von anderen erhalten (die Beispiele Sozialfürsorge und Versicherungen wurden schon erwähnt), ohne daß der Gesichtspunkt, ob diese Informationen tatsächlich benötigt werden, eine Rolle spielt;
> - Art und Ausmaß des Geheimhaltungsinteresses auf Seiten der Patienten nicht empirisch belegt sind (der freimütige Umgang mit Informationen über die eigene Gesundheit widerspricht manchen Äußerungen der ärztlichen Standesorganisa-

[391] Dammann (1973). Es handelt sich um ein Geoinformationssystem, das das Land Hessen bis heute betreibt.
[392] Dammann (1973, S. 257 ff.). Siehe auch Marwedel (1973), der als Leiter der Datenzentrale Schleswig-Holstein ein ähnlich aufgebautes System beschreibt, das aus den gleichen Quellen gespeist wird, ohne dabei ein Wort zu den möglichen negativen Folgen für Individuum und Gesellschaft zu verlieren. Fast noch spannender ist die Werbung auf der Seite vor Marwedels Artikel: „INPOL ist ein gutes Beispiel für die Leistungssteigerung der Polizei… … und für das universell einsetzbare Siemens-System 4004."
[393] Dammann (1973, S. 269 f.).
[394] Rave (1973).
[395] Rave (1973, S. 279).
[396] Rave (1973, S. 280).

> tionen über Geheimhaltungsbedürfnisse, deren Verletzung ein unverzichtbares Vertrauensverhältnis zerstören soll).“[397]

Wolfgang Kilian analysiert in seinem Beitrag die Fragen des Datenschutzes, die sich im Bereich der Wirtschaft stellen.[398] Er verweist darauf, dass das Datenschutzproblem keineswegs neu sei, Anlass für eine grundsätzliche Neuregelungen des gesamten Feldes allerdings die technische Entwicklung bei der automatisierten Informationsverarbeitung und deren Möglichkeiten zum Sammeln, Aggregieren, Strukturieren, Auswerten und Weitergeben von Daten gebe.[399] Kilian identifiziert drei Gruppen von Wirtschaftsunternehmen, von denen unterschiedlich große Gefahren ausgehen würden. Die größte Gefahr gehe von Unternehmen aus, bei denen die Information selbst die Ware darstellen. Für diese schlägt er vor, in einem Gesetz „zulässige und unzulässige Zwecke aufzuzählen.“[400] Die zweite Gruppe, die er identifiziert, umfasse solche Unternehmen, „deren Geschäftszweck nicht unmittelbar oder nur zum Teil im Handel mit Informationen besteht, die aber in besonders hohem Maße von personenbezogenen Daten abhängen“ wie etwa Banken und Versicherungen.[401] Die größte Gruppe bestehe aus Wirtschaftsunternehmen, „bei denen personenbezogene Daten ausschließlich der internen Organisation und als Voraussetzung eines davon unabhängigen Geschäftszwecks dienen.“[402] Ziel des Datenschutzes sei nicht ein Datenverbot, sondern die „Kontrolle oder Überwachung der Beschaffung und Verwendung von Daten.“[403] Allerdings fordert er, frau solle „für Verknüpfungen das Verbotsprinzip gesetzlich festlegen.“[404] Abschließend weist Kilian darauf hin, dass die damaligen Entwürfe für ein BDSG bei Verletzung von Datenschutzbestimmungen keine zivilrechtlichen Ersatzansprüche vorsehen würden. Damit gelte für mögliche Schadensersatzansprüche das allgemeine Deliktsrecht, das Verschulden voraussetze. Dies sei allerdings bei Verwendung von IT-Systemen schwer nachzuweisen. Er schlägt daher die Einführung einer Gefährdungshaftung vor, wie sie etwa auch im schwedischen Entwurf zu einem Datenschutzgesetz enthalten sei.[405]

Kilian ist einer der Wenigen, die die Datenschutzdiskussion selbst beobachten und deren inhärente Verwerfungen identifizieren können:

> „Die Datenschutzdiskussion mag für Außenstehende oft den Eindruck erwecken, als versuchten einige Juristen mit den ihnen zur Verfügung stehenden Mitteln den technischen Fortschritt zu hemmen. Der Eindruck ist deshalb schwer zu zerstreuen, weil es an praktischen Beispielen für die verbundenen Gefahren mangelt und alle Datenschutzvorschläge mehr oder weniger auf Vermutungen über künftige Auswirkungen von Informationssystemen beruhen. Andererseits darf nicht gewartet werden, bis sich erkennbare Gefahrenlagen aktualisieren, weil dies dann gleich tausendfach geschehen und die Entwicklung nur schwer oder gar nicht mehr rückgängig gemacht werden kann. Gerade solche Juristen, die sich intensiv mit EDV beschäftigen, weisen darauf

[397] Rave (1973, S. 286 f.). Siehe dazu auch die spätere Diskussion zum sogenannten Privacy-Paradox.
[398] Kilian (1973).
[399] Kilian (1973, S. 293).
[400] Kilian (1973, S. 297).
[401] Kilian (1973, S. 294).
[402] Kilian (1973, S. 299).
[403] Kilian (1973, S. 289). Auch „Datenverwendungskontrolle“, siehe S. 301.
[404] Kilian (1973, S. 304).
[405] Siehe Kilian (1973, S. 308). Siehe dazu auch die weitergehende Forderung nach einer Beweislastumkehr zugunsten der Betroffenen, die Josef Gärtner zusätzlich zur Forderung nach einer Gefährdungshaftung erhebt, Gärtner (1976, S. 71 ff.).

> immer wieder hin. Sie haben die Hoffnung, daß aufgrund der Datenschutzdiskussion künftig schon bei der Entwicklung neuer Informationssysteme die Implikate und Konsequenzen für den einzelnen Bürger mitbedacht werden.“[406]

Eine dezidiert andere Vorstellung vom Datenschutz äußerte Simitis,[407] der von der Annahme ausgeht, dass die staatliche Administration, die sich selbst als leistende und planende Verwaltung verstehe, „tendenziell auf Totalinformation ausgerichtet“ sei, „mag im übrigen von der Persönlichkeit und ihrem Schutz noch so viel die Rede sein.“[408] Auch für das Individuum habe sich die Situation in der „industriellen Gesellschaft“ grundlegend geändert: Es stelle sich der Einzelnen gar nicht mehr „die Frage nach der Exklusivität seiner Privatsphäre.“ Was ihn allein interessiere, seien die Leistungen, auf die sie angewiesen sei. Diese Leistungen seien aber gar nicht anders zu erhalten als über „die Bereitschaft zur Information.“[409] Verhindert werden solle, dass „Informationsbeschaffung und Informationsverarbeitung den einzelnen [...] vollständig funktionalisieren und zum schlichten Objekt staatlicher und privater Bürokratie degradieren.“[410] Deshalb liege die spezifische Gefahr auch nicht „im Mißbrauch der gespeicherten Angaben.“ Entscheidend sei vielmehr „die mit dem Übergang zu einem qualitativ neuen Informationsinstrumentarium angestrebte Perfektionierung der sozialen Steuerung.“[411] Simitis schließt daraus, dass Information nicht beliebig verfügbar sein dürften und ihr Gebrauch der Legitimierung und Kontrolle bedürfe. Mit seinem Hintergrund als Arbeitsrechtler und den Erfahrungen mit dem kollektiven Arbeitsrecht sieht er die Funktion des Datenschutzes in der Schaffung von „institutionalisierte[n] generelle[n] Barrieren [...], die Abwehr also nicht mehr der individuellen Möglichkeit überläßt.“[412] Der Kern aller Datenschutzregelungen sei „kalkuliertes Nichtwissen.“[413] Simitis hält das Datenschutzproblem für ein ausschließlich im Zusammenhang mit der Verwendung elektronischer Anlagen auftretendes Phänomen. So dürfte frau „umsonst [...] nach Vorschriften für diese [manuelle] Form der Datenverarbeitung suchen.“[414]

Simitis lehnt eine Ausdehnung des Datenschutzes über den Einzelnen hinaus ab.[415] Peinlich ist allerdings die Begründung: Weil es die ersten Datenschutzgesetze und Gesetzentwürfe so bestimmen.[416] Darüber hinaus negiert er die Existenz von Informationsmachtgefällen, an deren unterem Ende eine Organisation steht.[417] Zugleich verfolgt er offen das Ziel, das Menschenrecht auf ein Bürgerinnenrecht zurechtzustutzen.[418]

Sein Vorschlag für einen Lösungsansatz orientiert sich nicht wie bei Steinmüller und seinen Mitautorinnen am prototypischen Informationsverarbeitungsprozess, obwohl er deren Arbeit rezipiert, sondern an den Daten und ihren Verwendungszusammenhängen. Deren funktionale Analyse sichere ein Höchstmaß an Flexibilität, und weil der Verwendungszusammenhang im Mittelpunkt stehe, könnten sich die rechtlichen Regelungen „am konkreten Konflikt orien-

[406] Kilian (1973, S. 305).
[407] Simitis (1973)
[408] Simitis (1973, S. 144).
[409] Simitis (1973, S. 145).
[410] Simitis (1973, S. 147).
[411] Simitis (1973, S. 147, Fn. 32).
[412] Simitis (1973, S. 148).
[413] Simitis (1973, S. 154).
[414] Simitis (1973, S. 167). Das liegt allerdings an seiner beschränkten Datenschutzdefinition. Da war die Diskussion damals schon lange weiter. Siehe auch von Lewinski (2009).
[415] Simitis (1973, S. 154 ff.).
[416] Simitis (1973, S. 154, Fn. 51).
[417] Simitis (1973, S. 156).
[418] Simitis (1973, S. 158).

tieren.“[419] Daher spricht er sich auch gegen Versuche aus, das Datenschutzproblem in einem einzelnen Gesetz zu regeln: Zu verschieden seien die Verwendungszusammenhänge, kaum vergleichbar Position und Situation der einzelnen Adressaten einer Datenschutzregelung, mit einer Vielzahl von zu berücksichtigenden Interessenkollisionen.[420] „Der exzessive Gebrauch von Generalklauseln ist die Kehrseite der mangelnden, ja unmöglichen Differenzierung.“[421] Er plädiert stattdessen für die ausschließliche Verwendung bereichsspezifischer Regelungen.[422] Durchsetzen lasse sich Datenschutz, so Simitis, nur durch Fremdkontrolle.[423] Und internationaler Datenaustausch, der damals durchaus schon weit verbreitet war,[424] sei nur solange akzeptabel, wie auch der Datenschutz internationalisiert werde.[425]

Während Seidel in seiner im Vorjahr erschienenen Arbeit über den Umgang mit personenbezogenen Informationen in Datenbanken umfassend auf Beispiele sowohl aus den USA als auch aus der BRD verweist, dabei vom Kreditauskunftswesen über Adressverlage und Personaldatenbanken bis hin zu statistischen und sozialwissenschaftlichen Datenbanken thematisch eine große Breite abdeckt und Gefahren wie die Bildung von Persönlichkeitsprofilen, die Möglichkeiten zu politischer Überwachung sowie Schwarze Listen in verschiedenen Bereichen identifiziert, beschreiben Klaus Tiedemann und Christoph Sasse eine Welt, in der es eine scharfe Trennung zwischen der schrecklichen Realität in den USA mit ihren bösen Kreditauskunfteien und der heilen Welt mit den guten Auskunfteien in der BRD gebe.[426] Mit Beispielen, die vor allem Wirtschaftssubjekte betreffen, nicht jedoch Verbraucherinnen, versuchen die Autoren unter anderem die Schufa pauschal zu exkulpieren, obwohl diese bis 2006 ausschließlich über Verbraucherinnen Auskunft erteilte. Insbesondere für Auskunfteien positive Aussagen in dem als Gefälligkeitsgutachten zu bezeichnenden Werk stammen ausschließlich von diesen selbst oder sind unbelegt.[427] Einzig die Auswertung der bis zu diesem Zeitpunkt in der BRD erschienenen Literatur zum Datenschutz ist positiv hervorzuheben, wenn auch eher wegen ihres Umfangs als wegen ihrer Objektivität.[428] Alle „düstere[n] Prognosen einer einseitigen Literatur professioneller Datenschützer“[429] sind tatsächlich eingetreten, wenn auch in einigen Fällen erst Jahre oder Jahrzehnte „verspätet“, während alle Schönredereien und Beschwichtigungen von Tiedemann und Sasse sich im Nachhinein bestenfalls als Irrtum, manchmal auch als Lüge herausstellten.

Podlech veröffentlichte 1973 seinen zuvor angekündigten Entwurf für ein Bundesdatenschutz-Rahmengesetzes samt Begründung.[430] Herausragende Eigenschaft dieser Arbeit ist, dass Podlech – im Gegensatz zu Steinmüller und seinen Mitautorinnen – seine Annahmen so umfassend wie möglich aufdeckt.[431] Inhaltlich beschränkt er sich auf den Datenschutz im öffentlichen Bereich,

[419] Simitis (1973, S. 154).
[420] Simitis (1973, S. 182 f.).
[421] Simitis (1973, S. 184).
[422] Simitis (1973, S. 186).
[423] Simitis (1973, S. 174).
[424] Das war gerade der Grund, warum sich die OECD für gleiche – und gleich niedrigschwellige – Datenschutzregelungen einsetzte, siehe Niblett (1971).
[425] Simitis (1973, S. 182).
[426] Tiedemann und Sasse (1973).
[427] Siehe etwa die Aussage zur Höhe der Dunkelziffer bei Krediterschleichungen, S. 8, oder zur Art und zum Umfang der über Betroffene erhobenen und weitergegebenen Daten, S. 46.
[428] Siehe Tiedemann und Sasse (1973, S. 89 ff.). Zur Objektivität siehe auch die Wortwahl auf den Seiten 18 ff. und 36 ff.: Während das Verhalten von Kreditnehmerinnen pauschal als „kriminell“ bezeichnet wird, gilt das gleiche Verhalten bei Auskunfteien beschönigend als „Mängel“ und „Mißstände“.
[429] Tiedemann und Sasse (1973, S. 107).
[430] Podlech (1973a).
[431] Das Werk ist damit zwar sehr schwer zu lesen, aber auch sehr gehaltvoll.

da er sich für nicht ausreichend kompetent erachtete, auch für den Bereich der Wirtschaft entsprechende Regeln auszuarbeiten.[432]

Zu Beginn schlägt Podlech eine Änderung des Grundgesetzes mit dem Ziel vor, dem Bund die Kompetenz für eine bundeseinheitliche Regelung des Datenschutzes zu verleihen.[433]

Der Gesetzentwurf enthält nach Abschnitten mit Begriffsbestimmungen und allgemeinen Vorschriften sieben inhaltliche Abschnitte sowie einen Abschnitt mit Schlussbestimmungen. Letztere enthalten Änderungen für andere gesetzliche Regelungen, die sich aus der Einführung eines Datenschutzgesetzes ergeben.[434]

Bevor Podlech die einzelnen Vorschläge erläutert, gibt er einen Überblick über den Stand der Gesetzgebungsarbeiten auf dem Gebiet des Datenschutzes und identifiziert die Eigenschaften, die existierende Datenschutzvorschriften und -entwürfe kennzeichnen.[435] Alle Entwürfe gingen aus „von der Privatsphäre des Einzelnen und versuchen zu verhindern, daß Informationen aus dieser Privatsphäre unberechtigt verwendet werden.“[436] Dabei werde weder die Privatsphäre selbst näher umschrieben noch finde eine Auseinandersetzung mit der zu diesem Begriff kritischen Literatur statt.[437] Anschließend beschreibt Podlech die Ausgangslage sowie die daraus für seinen Entwurf resultierenden Folgerungen.[438] Er geht von den Planungen der Länder und des Bundes für „umfassende integrierte Informationssysteme“ aus, „die alle Behörden und nahezu alle Staatsfunktionen umfassen“ würden.[439] Seiner Meinung nach seien zwar erstens umfassende Verknüpfungen ohne das bundeseinheitliche Personenkennzeichen noch nicht möglich und zweitens geheimdienstinteressante personenbezogene Daten noch kaum gespeichert,[440] aber es sei klar, dass wenn integrierte Informationssysteme erst einmal eingerichtet seien, es nahezu unmöglich sein werde, ihre grundlegende Struktur noch erheblich zu ändern. „Datenschutz muß aber bei der Struktur der Informationssysteme ansetzen.“[441] Da einzelne Schutzmaßnahmen jeweils für sich nicht ausreichten, da diese – ob technische, organisatorische oder rechtliche Schutzvorschrift – im einzelnen gebrochen werden könnten, bedürfe es einer sinnvollen Kombination dieser Maßnahmen mit begleitender Kontrolle.[442] An erster Stelle stünden organisatorische Maßnahmen wie „die Trennung von Unternehmer und Benutzer integrierter Informationssysteme.“[443] Zweitens bedürfe es eines „von einer relativ neutralen Stelle durchgeführte[n] Programmschutz[es].“[444] Erst auf dieser Basis ließen sich wirksame Rechte der Betroffenen und Strafbestimmungen als

[432] Siehe Podlech (1973a, S. V).

[433] Siehe Podlech (1973a, S. 1 ff.). Für den Bereich der privaten Informationsverarbeitung hätte das keine Änderungen gebracht, aber Podlech wollte dem Bund auch die Kompetenz verleihen, den Ländern „insoweit einen organisatorischen Rahmen vorzuschreiben, als es zur Sicherung eines effektiven Datenschutzes erforderlich ist.“ Siehe S. 4. Mit dem gleichen Argument hat die EU-Kommission für ihren Entwurf für eine Datenschutzgrundverordnung als Ersatz für die Datenschutzrichtlinie von 1995 geworben.

[434] Neben verschiedenen Statistikgesetzen sind nach Podlech etwa die Reichsversicherungsordnung, das G-10-Gesetz, das Bundessozialhilfegesetz oder das BAföG änderungsbedürftig.

[435] Siehe Podlech (1973a, S. 33 ff.).

[436] Siehe Podlech (1973a, S. 34 f.).

[437] Siehe Podlech (1973a, S. 35).

[438] Siehe Podlech (1973a, S. 35 ff.).

[439] Siehe Podlech (1973a, S. 36).

[440] Beide Annahmen haben sich als falsch herausgestellt.

[441] Siehe Podlech (1973a, S. 38).

[442] Siehe Podlech (1973a, S. 38).

[443] Siehe Podlech (1973a, S. 38). S. 50: „[J]ede Benutzung der Anlage durch eine andere Behörde als den Unternehmer [kann] nahezu vollständig kontrolliert werden [...], während es nahezu keine Möglichkeit gibt, den Unternehmer der Anlage zu kontrollieren. Die rechtliche Folge dieses Umstandes müssen organisatorische Anforderungen an den Unternehmer sein [...].“

[444] Siehe Podlech (1973a, S. 38).

weitere Schutzmaßnahmen formulieren.[445] Anschließend präsentiert Podlech das dem Entwurf zugrunde gelegte organisatorische Modell,[446] das vor allem auf Arbeiten des frühen Luhmann basiert – vor dessen autopoietischen Wende 1984.

Da sich keine materiellen Kriterien finden ließen, die es für den gesamten Bereich der öffentlichen Verwaltung ermöglichten zu entscheiden, welche Informationen eine Behörde oder ein Behördenteil erheben, speichern, verarbeiten und nutzen dürfe, wählt Podlech als Ersatz einen verfahrensorientierten Ansatz.[447] Er verlangt dazu eine transparent durchgeführte Erforderlichkeitsprüfung für jede zur Aufgabenerfüllung notwendige Datenverarbeitung.[448] Die aus dieser Prüfung abzuleitenden Regelungen sollen nach Podlech techniknah sein, weil nur so ein effektiver Schutz zu gewährleisten sei. Daher seien auch die Regelungen seines Gesetzentwurfs techniknah. Dabei nimmt er an, dass auch durch weniger techniknahe Regelungen das Problem der Veralterung dieser Regelungen vor dem Hintergrund der technischen Entwicklung nicht ausgeschlossen werden könne. Gerade deshalb sei die Techniknähe der von ihm vorgelegten Regelungen auch angemessen. Darüber hinaus nimmt er an, dass Datenschutzregelungen etwa alle fünf Jahre von der technischen Entwicklung überholt würden.[449]

Nach Podlech soll das Datenschutzgesetz Personen schützen, „alle natürlichen Personen, juristischen Personen des Privatrechts und alle Personengruppen, die Träger von Rechten und Pflichten sein können."[450] Rechtlicher Anknüpfungspunkt sollen dabei personenbeziehbare Daten sein, also über die personenbezogenen hinaus auch solche, bei denen „geschickt gewählte Merkmalskombinationen" als Namensersatz dienen können,[451] die als statistische Angaben durch Zusatzinformationen wieder zu personenbezogenen Daten werden können oder pseudonymisierte Daten.[452]

Eine Besonderheit des Podlechschen Entwurfs liegt in der Ausnahme der Geheimdienste von den Datenschutzregelungen, „weil entweder eine Einhaltung der Vorschriften nicht kontrolliert werden kann oder die Kontrolle dazu führt, daß die Geheimdienste ihre Aufgaben nicht entsprechend den für Geheimdienste geltenden Regeln erfüllen können."[453]

Der vierte Abschnitt, in dem Podlech die Prinzipien der Erforderlichkeit und der Gesetzmäßigkeit der Informationserhebung und des Informationsaustausches regelt, ist der materielle Kern

[445] Siehe Podlech (1973a, S. 39).

[446] Siehe Podlech (1973a, S. 39 ff.). Der verfassungsmäßige Grundsatz der Gewaltenteilung wird ausgedehnt zum „Grundsatz der Systemdifferenzierung der öffentlichen Verwaltung", da „nur durch neue Konzeptionen die Wahrung der traditionellen Verfassungsprinzipien wie Rechtsstaat, Gewaltenteilung, Gesetzmäßigkeit der Verwaltung, Freiheitsspielräume der Bürger durch effektive Geltung der Grundrechte gewährleisten." (S. 39) An die Stelle einer „Einheit der Rechtsordnung" soll das „empirische Prinzip der Konkurrenz staatlicher Teilsysteme" treten, da in staatlich organisierten und technisierten Gesellschaften „Freiheitsspielräume der Bürger nur noch gewährleistet werden können, wenn einzelne Behörden oder Behördensysteme in der Erreichung von konsistent nicht mehr formulierbaren Staatszielen konkurrieren." (S. 40) „In technisierten Systemen mit Machtdifferenzen [...] sind Rechte im Spannungsfeld entgegengesetzter Interessen nur zu wahren, wenn Interessen einschließlich derer, zu deren Schutz Rechte formuliert sind, auf unterschiedliche Behörden abgebildet werden." (S. 40) „[J]edes soziale System, das nach vorgegebenen Regeln vorgegebene oder selbst gewählte Ziele verfolgt, [ist bereit], die vorgegebenen Regeln zu verletzen, um der Erreichung der Ziele wegen, wenn über eine hinreichend lange Zeit keine Kontrolle der Regelkonformität des Verhaltens erfolgt." (S. 40 f.).

[447] Siehe Podlech (1973a, S. 42 f.).

[448] Siehe Podlech (1973a, S. 42).

[449] Siehe Podlech (1973a, S. 43).

[450] Podlech (1973a, S. 47).

[451] Siehe Podlech (1973a, S. 47). „Die Schwierigkeit besteht darin, daß in der Regel nur im Einzelfall erkennbar ist, ob die Merkmalskombination Namensfunktion besitzt oder nicht."

[452] Siehe Podlech (1973a, S. 48).

[453] Siehe Podlech (1973a, S. 51 und § 7 Abs. 4, S. 9).

des Entwurfs.[454] Der Grundsatz der Erforderlichkeit ist dabei eng auszulegen, für die Erforderlichkeitsprüfung für Sekundärinformationen werden noch höhere Anforderungen definiert und Tertiärinformationen dürfen gar nicht erhoben werden.[455] Für den Informationsaustausch und die Informationsweitergabe an Private hat Podlech Regelungen aus dem IPA-Entwurf übernommen, die selbst wieder auf dem Mikrozensusurteil und dem Scheidungsaktenurteil des BVerfG basieren.[456] An eine mögliche Einwilligung stellt er hohe Anforderungen: „[D]ie Einwilligung darf nicht durch Allgemeine Geschäftsbedingungen vereinbart werden; sie ist unwirksam, wenn sie unter Ausnützung einer wirtschaftlichen Machtstellung erreicht wurde.“[457] Neben diese allgemeinen Regelungen stellt Podlech darüber hinaus besondere Anforderungen an den Informationsaustausch mit Hilfe von Computern.[458] So regelt er, dass in Datenbanken ein „künstliches Vergessen“ eingebaut werden muss.[459] Anschließend definiert er ein Verfahren, mit dem für die einzelnen Behörden und Behördenteile deren Aufgaben transparent gemacht werden, für die dann ermittelt werden kann, welche Informationen für deren Erfüllung erforderlich sind. Zu allen zu speichernden Informationen sind dann die Informationen mitzuspeichern, welche Behörden für die Erfüllung welcher Aufgaben in welcher Form darauf zugreifen und diese Daten verarbeiten, weitergeben oder nutzen dürfen.[460] Die rechtlichen Vorgaben sind dann in „Schutzprogramme“ zu übersetzen,[461] die zu veröffentlichen sind, damit sie öffentlich kontrolliert werden können, getestet und genehmigt werden müssen.[462] Für rechtswidrig erlangte Informationen stellt Podlech ein allgemeines Verwendungsverbot auf, das sich auch auf Verfahren vor Gericht bezieht und dort einem Verwertungsverbot enspricht, und „beendigt das Verfahren der V-Männer.“[463]

Da eine nachfolgende Kontrolle immer verhindert werden und sich auch eine vorbeugende Kontrolle durch „spätere unkontrollierbare Eingriffe in die Programme immer umgangen werden“ könne, funktioniere nur eine begleitende Kontrolle durch die Trennung von Unternehmung und Nutzung von Datenbanken.[464] Die Unternehmerinnen integrierter Informationssysteme – die Datenzentralen oder Informationsämter – sollen dabei nach dem Muster der Rechnungshöfe konstruiert sein und genauso unabhängig wie diese.[465] Sie stellen einen „organisatorischen Kunstgriff dar, um die Systemgliederung innerhalb der öffentlichen Verwaltung aufrechtzuerhalten, da integrierten Informationssystemen der öffentlichen Verwaltung die freiheitsbedrohende Tendenz innewohnt, Behördengrenzen funktional aufzulösen und Behörden alter Art zu Attrappen vor gesetzlich nicht ausgewiesenen Machtzentren werden zu lassen.“[466] Damit will Podlech

[454] Siehe Podlech (1973a, S. 54 ff.).
[455] Siehe Podlech (1973a, S. 55) Die Primärinformationen sind dabei diejenigen Informationen, die zur Erfüllung einer Aufgabe für eine Behörde erforderlich sind. Sekundärinformationen dienen der Plausibilitätsprüfung der Primärinformationen und Tertiärinformationen der Plausibilitätsprüfung von Sekundärinformationen.
[456] Siehe Podlech (1973a, S. 56 ff.).
[457] Siehe Podlech (1973a, § 16 Abs. 3 Nr. 2 Sätze 2 und 3, S. 12).
[458] Siehe Podlech (1973a, S. 59 ff.).
[459] In seiner Erläuterung bezieht er sich dabei auf den nichtexistenten § 19 Abs. 1 Nr. 4 seines Entwurfs.
[460] Siehe Podlech (1973a, S. 59).
[461] Siehe Podlech (1973a, S. 60). Ungefähr zur gleichen Zeit ist ein solcher Vorschlag das erste Mal in der IT-Sicherheits-Literatur erschienen, als „reference monitor“, siehe Anderson (1972, S. 22). Viel später wurde es dann von HP als „sticky policies“ patentiert.
[462] Siehe Podlech (1973a, S. 63). Da die Programme eine „erhebliche effektive Rechtswirkung“ entwickelten, müssten sie auch gerichtlich überprüfbar sein, siehe S. 65 ff.
[463] Siehe Podlech (1973a, S. 62).
[464] Siehe Podlech (1973a, S. 68 ff.).
[465] Siehe Podlech (1973a, S. 70).
[466] Siehe Podlech (1973a, S. 73).

die „Metafunktion öffentlicher Verwaltung“ unterstützen, die „auf die Garantie einer bestimmten Form der Erledigung von Verwaltungsaufgaben gerichtet ist.“[467]

Abschließend erläutert Podlech die den Betroffenen gewährten subjektiven Rechte,[468] die denen des IPA-Entwurfs entsprechen und auch im Vergleich mit anderen Vorschlägen aus dieser Zeit keine neuen Aspekte aufbringen.

Ein 1974 erschienener Debattenbeitrag von Ernst Benda, „Privatsphäre und »Persönlichkeitsprofil« – Ein Beitrag zur Datenschutzdiskussion“,[469] verdient nicht deshalb besondere Aufmerksamkeit, weil Benda neue Probleme aufzeigen, neue Argumente bringen oder neue Lösungsansätze in den Diskurs einbringen würde, sondern weil er in seiner letzten Entscheidung als Präsident des Bundesverfassungsgerichts – dem Volkszählungsurteil – dem Recht auf informationelle Selbstbestimmung als Grundrecht zum Durchbruch verhalf.[470] Benda stellt in seinem Beitrag nicht die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG, sondern die Menschenwürde nach Art. 1 Abs. 1 GG als dem obersten Wert in der Wertordnung des Grundgesetzes in den Mittelpunkt seiner Aufmerksamkeit, während er die Folgen der „Bürokratisierung des Staatsapparats“ für die „Möglichkeiten spontanen Verhaltens und autonomer Entscheidungen“ analysiert und bewertet.[471] Die neuen technische Möglichkeiten führten zu einer „neue[n] Qualität staatlicher Tätigkeit [...], welche die überkommenen Strukturen der öffentlichen Verwaltung radikal verändern“ würden mit der Folge, „daß die den Rechtsstaat schützenden Verfassungsnormen, die sich am klassischen Behördenverhalten orientieren, nahezu obsolet werden.“[472] Staatliche Verfassungsprinzipien müssten, um weiter wirksam sein zu können, „im Lichte einer ganz neuartigen Gefährdung interpretiert werden.“[473]

Nach Benda gehe die Datenschutzdiskussion „von der Befürchtung aus, daß der Bürger zum »Datenobjekt«“ und „in seinem Menschsein bedroht“ werde, „weil die Bürokratie mächtiger und undurchschaubarer wird und weil staatliche Planung den Menschen dem Plan anpassen und sich über sein »beschränktes Einsichtsniveau« hinwegsetzen könnte.“[474] Er behauptet, Ziel des Datenschutzes sei, „einen dem einzelnen gewährleisteten, dem Zugriff des Staates entzogenen Bereich abzugrenzen.“[475] Zwar grenzt er sich bei seiner Analyse von der vom Bundesverfassungsgericht vertretenen Sphärentheorie ab,[476] hält aber unter Verweis auf Westin und Jourard an der Vorstellung fest, Ziel der „Privatheit“ sei die Abgeschiedenheit, die Abtrennung von der Gesellschaft, quasi die Flucht vor der Gesellschaft.[477] Weil sich für Benda die „Privatheit“ im Rückzug aus der Gesellschaft erschöpft, kann sie dort nicht sein, wo der Mensch „im Bereich der Sozialsphäre tätig wird.“[478] Dem Menschen stehe daher in diesem Bereich weder ein generelles Recht auf in-

[467] Siehe Podlech (1973a, S. 73). Siehe dazu auch umfassend Luhmann (1969).
[468] Siehe Podlech (1973a, S. 75 ff.).
[469] Benda (1974).
[470] BVerfG (1983).
[471] Benda (1974, S. 23).
[472] Benda (1974, S. 25).
[473] Benda (1974, S. 25). Benda zitiert in diesem Zusammenhang neben Schelsky (1957) auch Steinmüller, Seidel, Westin/Baker und Podlech.
[474] Benda (1974, S. 27).
[475] Benda (1974, S. 28).
[476] Siehe Benda (1974, S. 29 ff.). Siehe aber auch sein Verweis auf die „Sozialsphäre“ bei der Begründung seiner Ablehnung eines – von niemandem geforderten, auch nicht von jenen, denen Benda das zuschreibt – „uneingeschränkte[n] »Selbstbestimmungsrecht[s]« des einzelnen“, S. 34.
[477] Siehe Benda (1974, S. 32). Benda zitiert hier Westin (1967) (in der Ausgabe von 1970) und Jourard (1966). Benda versucht damit erfolglos zu belegen, dass „das Recht auf Privatheit [...] nicht von einer angeblich überholten liberalen Vorstellung der Trennung von Staat und Individuum aus[geht].“
[478] Benda (1974, S. 34).

formationelle Selbstbestimmung noch auf „Selbstdarstellung“ zu, begrenzt werde die Erhebung, Speicherung und Verwendung der „Spuren“ aus „der Sozialsphäre“ oder „der Öffentlichkeit“ ausschließlich durch die Menschenwürde.[479] Das Recht auf informationelle Selbstbestimmung existiere „nur innerhalb der durch die Sozialbezogenheit des Menschen gezogenen Grenzen.“[480] Das eigentliche Problem stelle die Informationsintegration dar, die „dem Staat dann ein »Röntgenbild der Persönlichkeit« zur Verfügung“ stelle: „Die Möglichkeit, Persönlichkeitsprofile der Bürger anzulegen, verstärkt die Gefahr, daß der Staat den Menschen »in seiner ganzen Persönlichkeit« registriert und katalogisiert.“[481] Diese Vollabbildung der Persönlichkeit soll nach Benda „rechtlich und technisch“ unter Rückgriff auf das „soziologische[] Verständnis von »Privatheit« als einer »rollenspezifischen Informationsweitergabe« durch Individuen“ ausgeschlossen werden:

> „Der einzelne wird nicht so sehr dadurch in seiner Privatsphäre gefährdet, daß überhaupt Informationen über ihn existieren (zumal, da er selbst ständig bewußt oder unbewußt solche Daten vermittel); die eigentliche Bedrohung liegt darin, daß er die Verfügung darüber verliert, an wen und zu welchen Zwecken die Informationen vermittelt werden. Nicht die Informationen an sich, sondern ihre dysfunktionale Weitergabe, auf die der Betroffene keinen Einfluß hat, zerstört die Privatsphäre.“[482]

Benda widerspricht sich dabei selbst, nachdem er vorher noch behauptet hatte, dass diese Weitergabe hingenommen werden müsse, etwa als „Folgen eines wirtschaftlich unvernünftigen Verhaltens“ – womit er offenkundig auf die Kreditauskunfteien anspielt, die gerade von der Weitergabe der Informationen leben – oder als „soziale Sanktionen, wie das Unwerturteil anderer über ein zulässiges, aber fragwürdiges Verhalten“, die gerade auch auf der „dysfunktionalen Weitergabe“ von Informationen basieren.[483] Er zieht aus seiner Problematisierung noch nicht einmal die Konsequenz, „dem staatlichen Informationsbedürfnis absolute Grenzen wie etwa das Verbot der Bildung von »Persönlichkeitsprofilen« zu setzen.“[484] Allein das verfassungsrechtliche Verhältnismäßigkeitsprinzip soll „die Privatsphäre“ schützen.[485]

Eine konträre Position vertritt Walter Schmidt, der den Kern des Datenschutzes in der „bedrohten Entscheidungsfreiheit“ sieht: „Wer sich beobachtet weiß, stellt sich darauf ein. Wer durchschaut worden ist, dessen Verhalten kann im voraus abgeschätzt, dessen Entscheidungen können vorweggenommen werden.“[486] Beim Datenschutz gehe es weder nur um den „Schutz personenbezogener Daten“ noch ausschließlich um den Persönlichkeitsschutz. Auch sei ein Ausschluss von anonymisierten Daten angesichts ihrer Problematik falsch.[487]

Nach Schmidt stelle die Ausweitung der Verfügbarkeit personenbezogener Informationen, die sich zum „»Lebensbild« oder »Persönlichkeitsprofil«“ fügten, das grundlegende Problem dar: „Die bisher nur bestimmten Stellen gegenüber preisgegebene, damit allenfalls teilöffentliche und im übrigen weiter »private« Information wird jetzt insoweit (für alle Zugriffsberechtigten) voll

[479] Benda (1974, S. 34 ff.). So sei nicht zu beanstanden, wenn wie „in den Großstädten der USA routinemäßig alle Kraftwagenkennzeichen mit Hilfe der EDV daraufhin überprüft [werden], ob sich unter den erfaßten Wagen gestohlene Fahrzeuge befinden.“ (S. 35).
[480] Benda (1974, S. 35 f.).
[481] Benda (1974, S. 37).
[482] Benda (1974, S. 37).
[483] Vergl. Benda (1974, S. 34).
[484] Benda (1974, S. 41).
[485] Benda (1974, S. 40, 44).
[486] Schmidt (1974, S. 241).
[487] Schmidt (1974, S. 241).

»öffentlich«.“[488] Deshalb könne ebenso gut von „Ent-Privatisierung“ wie von „Ver-Öffentlichung“ gesprochen werden. Es werde, so Schmidt unter explizitem Rückgriff auf die überkommende Terminologie, eine „künstliche »Öffentlichkeitssphäre« des einzelnen“ erzeugt, über die sie nicht mehr selbst verfügen könne und die ihre „»Privatsphäre« aufhebt.“[489]

Wie auch schon Kamlah und Seidel wählt Schmidt den Ansatz der Analyse der „denkbaren Verletzungen“ als Ergänzung zu einer Klärung des „im einzelnen umstrittene Ziel des Persönlichkeitsschutzes (seinen »Gegenstand«)“.[490] Da Datenintegration die Verfügung über die zu integrierenden Daten voraussetze, müssten sich die Schutzvorkehrungen gegen die Datenintegration „in das Vorfeld der Informationsermittlung“ verlagern.[491] Weil sie sowohl für die staatliche wie die private Informationsverarbeitung „in den weitaus meisten Fällen an der sozialen Abhängigkeit“ vorbeigehe, sei die „»Freiwilligkeit« der Auskunft“ keine akzeptable Rechtfertigung eines Auskunftsverlangens.[492]

Als Ziele des Persönlichkeitsschutzes stellt Schmidt zwei Konstruktionen einander gegenüber: einerseits die „»Sphären«-Konstruktion und [den] Autonomieschutz“, andererseits die Entscheidungsfreiheit als „private und politische Autonomie“.[493] Das Sphärenmodell lehnt er begründet ab:[494]

> „Die Konstruktion abgestufter »Sphären« des Persönlichkeitsschutzes ist nur dann sinnvoll, wenn sich mit ihrer Hilfe ein für allemal brauchbare, jeweils im voraus einsetzbare Kriterien zur Abgrenzung des rechtlich geschützten von einem ungeschützten (Rest-?)Bereich finden lassen, mit anderen Worten, wenn sie einigermaßen sichere Maßstäbe liefert, die Inhalt und Umfang des Persönlichkeitsschutzes vorhersehbar machen. Gerade das ist ihr nicht gelungen und konnte ihr nicht gelingen. Weite Bereiche des gesellschaftlichen und des Berufslebens verschwimmen »im Zwielicht einer 'privaten' Öffentlichkeit«.“[495]

Schmidt sieht das Problem der Sphärentheorie in einer überkommenen Gesellschaftsvorstellung von Privatautonomie und schlägt daher einen anderen Weg vor:[496] „Statt eines sich selbst verwirklichenden objektiven Prinzips (der Privatautonomie) wird nunmehr die Selbstverwirklichungschance des (autonom gedachten) Subjekts geschützt.“[497]

> „Die integrierte Verarbeitung personenbezogener Daten ermöglicht individualbezogen die technische Reproduzierbarkeit des »inneren« Persönlichkeitsprofils und gruppenbezogen die Simulation des Konsumenten- und Wählerverhaltens, diese auch dann, wenn die Daten anonymisiert worden sind, also keinen Rückschluß mehr auf eine bestimmte Person [...] zulassen. [...] Der offenen und der anonymisierten Datenintegration ist gemeinsam, daß sie die persönlichen Entfaltungsmöglichkeiten jedes einzelnen schmälern und seine Abhängigkeit steigern. Die Reproduzierbarkeit seines Persönlichkeitsprofils trifft ihn stärker in seiner individuellen Abhängigkeit

[488] Schmidt (1974, S. 242).
[489] Schmidt (1974, S. 242).
[490] Schmidt (1974, S. 242 f.).
[491] Schmidt (1974, S. 242).
[492] Schmidt (1974, S. 243).
[493] Schmidt (1974, S. 243 ff.).
[494] Schmidt (1974, S. 243 ff.).
[495] Schmidt (1974, S. 243 f.), unter Verweis auf Maass (1970, S. 26).
[496] Schmidt (1974, S. 245).
[497] Schmidt (1974, S. 241).

> als Arbeit- und Kreditnehmer oder als Empfänger öffentlicher Leistungen; die Simulation eines Gruppenverhaltens trifft auch jedes einzelne Gruppenmitglied in seinen Entscheidungsmöglichkeiten als Konsument von Waren- oder Dienstleistungen oder als Element der politischen Willensbildung. [...] Diese hier nur grob skizzierten Möglichkeiten der Verhaltenssteuerung zeigen, daß es nicht länger genügen kann, bestimmte Lebensbereiche zu Freiräumen zu erklären und die Entscheidungsfreiheit des einzelnen, die erst solche »Schutzsphären« mit Leben zu erfüllen vermöchte, wie selbstverständlich vorauszusetzen. [...] Diese Entscheidungsfreiheit gilt es gegenüber Staat und Privatwirtschaft zu schützen; der einzelne bedarf mithin der privaten wie der politischen Autonomie."[498]

Entscheidungsfreiheit setze dabei „die Möglichkeit des Auch-anders-könnens" voraus, „mögliche Fremdsteuerungen des Entscheidungsverhaltens" müssten abgewehrt werden, es gehe um die Ausweitung der „Selbstbestimmungs- und Selbstverwirklichungsmöglichkeiten", also um die „Emanzipation". Informationsfreiheit und freie, ungehinderte Kommunikation seien daher grundlegend für eine Entscheidungsfreiheit. Auch seien nach öffentlichem wie privatem Recht „die »innere« Entscheidungsfreiheit ebenso zu schützen wie sie Selbstdarstellung nach außen."[499]

Der Schutz schließe dabei Informationen aus offen zugänglichen Informationsquellen notwendig mit ein. Die herrschende Meinung verfehle mit ihrem Versuch einer Abgrenzung einer „»Privatsphäre« von einer rechtlich ungeschützten »Öffentlichkeitssphäre«" das Problem: „[D]urch die Fixierung auf das Kriterium des »Privaten« hat sie den Schutz der politisch verstandenen Freiheit aus dieser Problemdiskussion hinausdefiniert."[500] In einem demokratischen Staat, „der von der Öffentlichkeit und durch die Öffentlichkeit" lebe, sei kaum etwas so empfindlich wie diese „»Öffentlichkeitssphäre«".[501] Das gelte auch für die private Informationsverarbeitung, „[a]ndernfalls wäre die politische Entscheidungsfreiheit eines jeden einzelnen durch Rücksichtnahme auf sein privates Fortkommen (als Arbeitnehmer wie als Unternehmer im Konkurrenzkampf) ständig bedroht – von der Umgehungsmöglichkeit für öffentliche Stellen [...] ganz zu schweigen, die sich lediglich privatrechtlicher Organisationsformen zu bedienen brauchten."[502] Schmidt fordert daher in Anlehnung an und Ergänzung zum Recht am eigenen Bild ein „Recht am Persönlichkeitsprofil".[503]

Zwar sei der Informationsaustausch das Kernproblem des personenbezogenen Datenschutzes, dieser könne aber erst gelöst werden, wenn vorher die Frage, wer welche Informationen zu welchen Zwecken erheben und speichern dürfe, gelöst sei: „[N]ur ein rechtmäßiger Datengebrauch aufgrund rechtlich unbedenklicher Informationsbeschaffung kann gegen Mißbrauch abgesichert werden."[504] Dabei seien nicht die technischen Möglichkeiten Maßstab für die Verarbeitung: „Die »Normalität« der anschwellenden Informationsflüsse erlaubt noch nicht den Schluß auf die *Norm*-alität jeder Art Informationssammlung und -verarbeitung."[505]

Ende 1972 entstand am Rande eines öffentlichen Hearings des BMI zum Referentenentwurf für ein Bundesdatenschutzgesetz die Idee, dass die Soziologinnen und Juristinnen, die als Sach-

[498] Schmidt (1974, S. 245 f.).
[499] Schmidt (1974, S. 246). Viel später auch – ohne aufzudecken, dass sie diese Vorstellung komplett übernommen hat – gleichlautend Britz (2007).
[500] Schmidt (1974, S. 247).
[501] Schmidt (1974, S. 247).
[502] Schmidt (1974, S. 248).
[503] Schmidt (1974, S. 248).
[504] Schmidt (1974, S. 248).
[505] Schmidt (1974, S. 248 f.).

verständige teilnahmen, einem größeren Publikum die Chancen und Gefahren elektronischer Datenbanken für Individuen und Gesellschaft zu verdeutlichen und dabei die Beschränkungen, die die „Diskussion von Regierungsbeamten, Lobbyisten und einzelnen Wissenschaftlern“ kennzeichne, zu überwinden.[506]

Im ersten Kapitel in dem 1974 erschienenen Werk gibt Ulrich Dammann einen Überblick über den Stand der wichtigsten Automatisierungsprojekte der bundesdeutschen Verwaltung. Neben der allgemeinen Verwaltungsautomation, die von der Automatisierung von Massen- und Routineaufgaben bis hin zu den damals sogenannten „Management-Information-System[en]“ [sic!] reichen, betrachtet er einige der Projekte näher: das „automatisierte Einwohner-Informations-System“, die bevorstehende – aber dann nicht gekommene – Einführung eines allgemeinen Personenkennzeichens sowie die polizeilichen und nachrichtendienstlichen Informationssysteme. Abschließend gibt er einen Überblick über das geplante „Informationsbankensystem“. Zu jedem der vorgestellten Systeme beschreibt Dammann dann die Möglichkeiten und Gefahren aus der Sicht des Datenschutzes.[507]

Steinmüller und Henner Wolter beschreiben im zweiten Kapitel die Besonderheiten elektronischer Datenverarbeitung gegenüber den „»herkömmlichen« Verfahren der Informationsverarbeitung, die mehr und mehr durch die EDV ersetzt werden.“[508] Die EDV wird dabei als System verstanden, „einem konkreten sozialen System [...], als dessen Teilsystem ein Mensch-Maschine-System fungieren kann.“ Es gehe also bei der Betrachtung des Datenschutzes nicht nur um Mensch-Maschine-Systeme oder gar nur die Maschine, den Computer.[509] Immer müsse analysiert werden, welchen Interessen ein konkretes Informationssystem objektiv nütze, welchen es schade.[510] Die Besonderheiten der automatisierten gegenüber der menschlichen – oder manuellen – Informationsverarbeitung liegen in der Erhöhung der Effizienz, der schnelleren Anpassung der Organisation an eine veränderte Umwelt bei gleichzeitig stärkerer Unabhängigkeit gegenüber dieser Umwelt, der Erhöhung der Zuverlässigkeit, der Steigerung der Lernfähigkeit der Organisation sowie die Fähigkeit zur Steigerung der zu verarbeitenden Komplexität.[511] Steinmüller und Wolter sehen in der Automatisierung der Verwaltung die Tendenz zur Integration und Zentralisation und im Ergebnis eine Ausweitung der Macht der Datenverarbeiter.[512]

Im dritten Kapitel versucht Paul J. Müller, eine soziologische Definition dessen anzugeben, „was als Privatsphäre von Personen anzusehen ist“ und welchen Gefahren sie ausgesetzt ist, bis hin zur Gefahr ihrer völligen Aufhebung.[513] Als allgemeine Definition von Privatsphäre gibt er an: „Sie wird durch Lebensbereiche von Individuen ermöglicht, in denen sie handeln können, ohne daß eine für sie dysfunktionale (nachteilige) Informationsweitergabe an andere erfolgt.“[514] Er trennt dabei, wie in der Soziologie üblich,[515] zwischen der Sichtbarkeit von Individuen für andere Individuen auf der einen und der Sichtbarkeit von Individuen für Institutionen.[516] Für die

[506] Dammann et al. (1974, Vorwort, o. S.).
[507] Siehe Dammann (1974a).
[508] Steinmüller und Wolter (1974, S. 51).
[509] Steinmüller und Wolter (1974, S. 52).
[510] Steinmüller und Wolter (1974, S. 53).
[511] Steinmüller und Wolter (1974, S. 54 ff.).
[512] Steinmüller und Wolter (1974, S. 58 ff.).
[513] Müller (1974).
[514] Müller (1974, S. 65).
[515] Die Nichtexistenz einer solchen Trennung bei der Beschreibung von Sozialbeziehungen weist auf ein fundamentales Fehl- oder Nichtverständnis gegenüber den soziologischen Grundlagen und damit auf die Untauglichkeit der jeweils angegebenen Privatsphären- oder *privacy*-Definition hin.
[516] Siehe Müller (1974, S. 65 ff.).

Beschreibung und Analyse „der Struktur der Kontakte des Menschen in seiner sozialen Umwelt“ und der daraus folgenden unterschiedlichen Sichtbarkeit gegenüber anderen Individuen – Mikro-Ebene – nutzt Müller die soziologische Rollentheorie. Dabei zeigt er unter anderem, inwieweit sich die Struktur der Sichtbarkeit etwa zwischen der mittelalterlichen Dorfgemeinschaft und der modernen Industriegesellschaft unterscheiden.[517] Anschließend präsentiert Müller einige empirische Befunde zur Sichtbarkeit von Individuen in ihren Umwelten.[518] Der zweite Teil beschäftigt sich mit der Sichtbarkeit von Individuen gegenüber Institutionen, d. h. der Makro-Ebene.[519] Dabei stellt Müller fest, dass es „eigentlich kaum noch Aktivitäten gibt, die keine Spuren bei Verwaltungen hinterlassen“ und alle diese Aktivitäten informationell abgebildet werden.[520] Die Dysfunktionalität der Informationsweitergabe lasse sich damit bestimmen als die „Aufhebung des Effektes von rollenspezifischer Informationsweitergabe der Individuen durch intermediäre Instanzen.“[521] Integrierte Informationsbankensysteme ermöglichten damit die Integration vormals differenzierter Rollen. „Die Forderung nach Integration von Information spiegelt vorindustrielle Lebensbedingungen wider, indem immer noch davon ausgegangen wird, das »Eigentliche« der Person sei durchgängig die Totalität aller Rollenerfüllungen, die »synthetische Person«.“[522] Kurz: Es handelt sich vor dem Hintergrund moderner, funktional differenzierter Gesellschaften, in denen wir leben, um eine rückwärtsgewandte Vorstellung.[523]

Mark O. Karhausen beschreibt im vierten Kapitel, welche Probleme sich in der empirischen Sozialforschung, die enorme Mengen personenbezogener Daten erhebt, verarbeitet und nutzt, ergeben und wie die Sozialforschung mit diesen Problemen umgeht.[524] Nach einer Einführung in Datenbanken im Allgemeinen und Umfragedatenbanken im Besonderen versucht Karhausen, die Schutzwürdigkeit von Informationen zu bestimmen, die er als „»Vertraulichkeit«“ bezeichnet.[525] Er unterscheidet dabei zwei Gründe, die die Vertraulichkeit von Informationen bestimmen würden: ein Interesse der Betroffenen und Normen und Wertvorstellungen der Gesellschaft. Es sei aber oftmals schwer zu entscheiden, ob bestimmte Informationen vertraulich sein sollen oder nicht. „Eine Lösung des Konflikts könnte in der Forderung bestehen, personenbezogene Daten generell als vertraulich und damit schutzwürdig zu behandeln.“[526] Abschließend beschreibt er bereits eingesetzte und mögliche weitere Methoden, Datenschutz in der empirischen Sozialforschung umzusetzen:[527] Anonymisierung und Pseudonymisierung, Zugangsbeschränkungen, frühe Kategorienbildung[528] und getrennte Speicherung unterschiedlicher Merkmale, etwa demographischer Merkmale und erhobener Meinungen oder Einstellungen. Neue Ansätze betreffen

[517] Siehe Müller (1974, S. 70 f.). Die moderne industrielle oder post-industrielle Gesellschaft ist mit der vorindustriellen Dorfgemeinschaft auch dann nicht zu vergleichen, wenn ihr der falsch verstandene Begriff des „global village“ umgehängt wird. Siehe dazu auch McLuhan (1962, S. 31).

[518] Siehe Müller (1974, S. 72 ff.).

[519] Müller (1974, S. 78 ff.).

[520] Siehe Müller (1974, S. 80).

[521] Müller (1974, S. 81).

[522] Müller (1974, S. 82).

[523] Siehe auch Pohle (2012).

[524] Karhausen (1974).

[525] Siehe Karhausen (1974, s. 99 ff.). Es handelt sich dabei um den Vertraulichkeitsbegriff der Soziologie, der die „Exklusivität der Information bzw. Informationsweitergabe einer Person an andere Personen oder Institutionen“ bezeichnet (S. 99).

[526] Karhausen (1974, S. 102).

[527] Siehe Karhausen (1974, S. 106 ff.).

[528] Dabei werden frühzeitig Daten kategorial aggregiert, d. h. es werden Aussageklassen gebildet, die mehrere Einzelkategorien zusammenfassen, und die Daten werden nur nach den Klassen, nicht jedoch nach den Einzelkategorien differenziert erhoben und gespeichert.

etwa die Beschränkung bestimmter Nutzerinnenkreise auf bestimmte Analysetechniken, Verkettungsschranken oder Mindestgruppengrößen bei der Ergebnisausgabe.[529]

Im fünften Kapitel betrachten Wolfgang Schimmel und Steinmüller die rechtspolitische Problemstellung des Datenschutzes.[530] Nachdem sie die Dringlichkeit einer gesetzgeberischen Lösung begründet haben, beschreiben sie die drei zentralen Interessen in der Datenschutzdiskussion: Erstens müsse die Funktionsfähigkeit von Staat, Wirtschaft und Wissenschaft erhalten oder gar gesteigert werden. Zweitens sollten die Möglichkeiten der EDV maximal genutzt werden. Und drittens sollten die gesellschaftlichen Freiheitsräume durch die Entwicklung der Informationstechnologie nicht gefährdet werden. Dies nennen sie das „magische Dreieck“ des Datenschutzes, die „»rein« vertreten“ einander ausschlössen.[531] Gleichwohl seien diese Interessen keineswegs gleichen Ranges: Informationsverarbeitung diene der Benutzerin (öffentliche Verwaltung, Wirtschaft, Wissenschaft), die wiederum der Gesellschaft insgesamt wie ihren Teilen, insbesondere den Bürgerinnen, dienten.[532] „Vollständiger [...] lautet die Präferenzreihe: Datenverarbeitung im Dienst der Verwaltung sowie der Wirtschaft und der Wissenschaft, jedoch unter der politischen Entscheidung der Volksvertretung und der Kontrolle der Justiz, all dies jedoch letztlich im Interesse der Personen und Personengruppen, die die Gesellschaft ausmachen.“[533] Dem entgegen stünden weit verbreitete Auffassungen, die etwa „»Rationalisierung« als oberstes Ziel der Automation“ oder „Bequemlichkeit“ – „»Die Daten sollen laufen, nicht der Bürger«“ – postulierten oder „»Schutz gegen Datenschutz«“ forderten.[534] Einzig die Sozialforscherinnen mit ihrem ungeheuren Datenbedarf hätten es verstanden, „die einzig zutreffende Folgerung“ zu ziehen: „die Vorlage eines realistischen und zugleich praktikablen Datenschutzkonzeptes, das ihr nicht nur politisch unbehindertes Arbeiten ermöglicht, sondern das durchaus auch der Verallgemeinerung auf andere nichtwissenschaftliche Bereiche fähig ist.“[535] Anschließend rekapitulieren die Autoren die Datenschutzdiskussion in verschiedenen Ländern, den USA, Großbritannien, Norwegen und der BRD.[536] Dem folgt eine Kritik an den Ansätzen und Grundbegriffen der „bisherigen“ Datenschutzforschung: der „Privatsphäre“ und ihrer Relativität, der Relativität der „personenbezogenen Daten“[537] und dem „Informationsgleichgewicht“.[538] Die Autoren identifizieren vier „datenschutzrechtliche Gefahrenfelder“: das Individuum „als Objekt staatlicher und privater Datenverarbeitung“, die „Verplanung von Individuen als Folge des Einsatzes von Informationssystemen“, die „Verschiebung des Informationsgleichgewichts“ sowie die „Bedeutung der Information für eine demokratische Gesellschaft“.[539] Besondere Risiken würden unter faktischen Abhängigkeitsverhältnissen (Arbeitsverhältnis, Verbraucherinnenschutz, staatliche Leistungsverwaltung),

[529] Siehe Karhausen (1974, S. 108 ff.). Letztere entsprechen in etwa dem neueren Verständnis von k-Anonymität.

[530] Schimmel und Steinmüller (1974). Und sie erklären, warum es sich um ein rechtspolitisches, und nicht um ein rechtsdogmatisches Problem handelt und was daraus für das Vorgehen folgt (S. 113).

[531] Siehe Schimmel und Steinmüller (1974, S. 114).

[532] Siehe Schimmel und Steinmüller (1974, S. 114 f.).

[533] Schimmel und Steinmüller (1974, S. 116).

[534] Siehe Schimmel und Steinmüller (1974, S. 116).

[535] Schimmel und Steinmüller (1974, S. 117).

[536] Siehe Schimmel und Steinmüller (1974, S. 117 ff.).

[537] Es entscheide nicht „die Datenart »personenbezogener Informationen«, sondern die (nicht generell bestimmbare) Leistungsfähigkeit des Informationssystems. Damit versagt der bisher häufig gemachte Versuch, durch rechtliche Sonderbehandlung bestimmter »sensitiver« Personeninformationen das Datenschutzproblem generell zu lösen“ (S. 133).

[538] Siehe Schimmel und Steinmüller (1974, S. 129 ff.).

[539] Siehe Schimmel und Steinmüller (1974, S. 134 ff.). Vereinfacht: Der erste Punkt beschreibt die menschenwürdebezogenen Folgen, der zweite die Folgen für die Entscheidungsfreiheit, der dritte die Folgen für das Machtverhältnis zwischen bestimmten gesellschaftlichen Subjekten und der vierte Punkt beschreibt die Informationsfreiheit.

rechtlichen Unterordnungsverhältnissen (Eingriffsverwaltung und Sicherheitsorgane, sogenannte „besondere Gewaltverhältnisse“) sowie in besonderen Vertrauensverhältnissen (medizinische, rechtliche und wirtschaftliche Beratung, die „[f]reiwillige Weitergabe durch den Betroffenen in Unkenntnis des Ausmaßes der Verwertung der Daten“ sowie die „[b]esondere[n] Risiken moderner Kommunikations- und Informationsverarbeitungstechniken“).[540] Abschließend stellen Schimmel und Steinmüller die rechtlichen Grundlagen des Datenschutzes – vor allem die verfassungsrechtlichen – und den Regierungsentwurf zum Bundesdatenschutzgesetz vor und unterziehen letzteren einer vernichtenden Kritik.[541]

In einem Nachwort erläutert Erwin K. Scheuch den Datenschutz als Machtkontrolle.[542] Unter Verweis auf Parsons und Tönnies erläutert er den Unterschied zwischen Gemeinschaft und Gesellschaft und zeigt, wie „in hoch differenzierten Industriegesellschaften“ Menschen auf der Basis ihres Verhaltens – oder der Basis von Informationen über ihr Verhalten – von anderen Individuen oder Institutionen bewertet werden, und wie die Menschen darauf allgemein mit „selektiver Informationsweitergabe“ reagieren.[543] Dabei stellt er fest, dass je asymmetrischer eine soziale Beziehung sei, „umso negativer ist für das Individuum die Durchbrechung der selbstgewählten Selektivität der Mitteilungen über sich selbst.“[544] Scheuch warnt vor der Auffassung, der Datenschutz gegenüber staatlichen Institutionen sei das dringlichere Problem: „Diese Auffassung beruht auf einem Irrtum über die Macht verschiedener Arten von Institutionen gegenüber Individuen.“[545] Der Staat sei zwar mächtiger und habe das Monopol für die Anwendung von Zwangsmitteln, sei jedoch auch stärker durch die Rechtsordnung kontrolliert. Dabei bedeute ein Mehr an Informationen offensichtlich ein Mehr an Macht, insbesondere wenn dieses Mehr an Informationen asymmetrisch sei: „die betreffende Institution weiß mehr über den Bürger, dieser aber nicht mehr über die Interna der Institution.“[546] Daraus folge dann, dass „[d]as Korrelat zur Forderung nach Datenschutz für das Individuum [...] dann die zweite Forderung nach Zugang zu Informationen“ für die Bürgerinnen sei, „aber auch und vor allem für andere Institutionen.“[547] Es gehe also um den Kampf gegen Informationsmonopole, denn „[m]it den Datenbanken und allgemein den Informationssystemen gewinnen diejenigen Institutionen an Gewicht, die diesen Informationszuwachs für sich monopolisieren können.“[548]

Ende 1973 fand in Köln eine internationale Fachtagung der Gesellschaft für Informatik und des Betriebswirtschaftlichen Instituts für Organisation und Automation an der Universität zu Köln zum Thema „Informationszentren in Wirtschaft und Verwaltung“ statt. Anhand der Tagungsdokumentation lässt sich wegen der großen personellen Überschneidung mit den Akteurinnen der Datenschutzdebatte erkennen, in welchem gesellschaftlichen und Informationsverarbeitungskontext sie das Datenschutzproblem eingebettet sehen. Malte von Berg analysiert die Tendenz der Entwicklung der automationsgestützten Informationsverarbeitung in der öffentlichen Verwaltung hin zur Integration, zur Schaffung von Datenverbünden mit ihrer „Idealforderung nach einmaliger Ermittlung und Erfassung der Daten sowie ihrer beliebigen Verknüpfbarkeit“,[549] die insoweit zur Auflösung der „hoch differenzierte[n] überkommene[n] Verwaltungsstruktur“ füh-

[540] Siehe Schimmel und Steinmüller (1974, S. 137 f.).
[541] Siehe Schimmel und Steinmüller (1974, S. 140 ff.).
[542] Scheuch (1974).
[543] Siehe Scheuch (1974, S. 171 ff.).
[544] Scheuch (1974, S. 173).
[545] Scheuch (1974, S. 173).
[546] Scheuch (1974, S. 175).
[547] Scheuch (1974, S. 175).
[548] Scheuch (1974, S. 175).
[549] von Berg (1974, S. 70).

re.[550] Die sich daraus ergebenden Fragen der Zentralisierung, des Verhältnisses zur Bürgerin oder zur Legislative bedürften dann rechtspolitischer Steuerung.[551] Mit genau diesen Fragen der „Gewalten-(Macht-)begrenzung und -verschränkung“[552] und des Verhältnisses zur politischen Öffentlichkeit beschäftigt sich ausführlich Klaus Grimmer.[553] Erstere verstanden als „Begrenzung der Informations- und Entscheidungskompetenz“ lasse sich insofern technisch lösen, soweit sie eine „Begrenzung der Datenzugriffmöglichkeit“ betreffe,[554] darüber hinaus müssten die demokratischen und rechtsstaatlichen Verfassungsprinzipien durch eine angemessene organisatorische Institutionalisierung der Informationssysteme und die Regelung von Zugriffs-, Auskunfts- und Löschungsrechten sichergestellt werden.[555] Für das Verhältnis der informatisierten öffentlichen Verwaltung zu Gesellschaft und Bürgerin sieht Grimmer zwei mögliche Entwicklungsrichtungen:

> „Der Einsatz von IS kann auch die Stellung des Bürgers im politischen Meinungsbildungsprozess und bei der Teilhabe an Verwaltungsentscheidungen verändern. So kann ein IS zur Herstellung von »Öffentlichkeit« und damit also zur Herstellung von Kommunikations- und Partizipationsmöglichkeiten, zur »Demokratisierung« genutzt werden, indem durch bessere Information und Teilnahme an Informationsprozessen von Individuen und Gruppen, von politischen Organisationen, Presse und Rundfunk der »öffentliche Bereich« durch Publizität hergestellt wird, womit sich auch eine qualitative Veränderung des Kommunikationssystems, in welchem Verwaltung steht und beurteilt wird, ergibt. Andererseits kann der Einsatz eines solch umfassenden Hilfsmittels, wie es das IS darstellt, Qualität, Organisation und Funktion der Verwaltung in der Weise verändern, dass sich eine Entwicklung zum autoritär-technokratischen »Verwaltungsstaat« ergibt.“[556]

Die Gefahr von letzterem ergebe sich aus der Verselbständigung „des Systems Verwaltung gegenüber dem politischen System“,[557] dem – in Anlehnung an Forderungen Podlechs – nur begegnet werden könne, wenn „institutionell und organisatorisch zwischen Verwaltung als operativer (ordnender, leistender und planender Tätigkeit) und Informationsverwaltung getrennt“ werde.[558] Im Ergebnis würde die operative Verwaltung begrenzt und kontrolliert durch die Informationsverwaltung, der wiederum „keine Handlungs- und Entscheidungskompetenz gegenüber dem Bürger, also nach aussen“ gewährt werden dürften.[559] D. Rave analysiert die drei zentralen Ziele, die mit der Errichtung von Informationszentren in der öffentlichen Verwaltung erreicht werden sollen: Wirtschaftlichkeit, Integration und Transparenz, nach den dahinter stehenden Interessen.[560] Die ersten beiden Ziele, bei der Standpunkt der Innenbetrachtung der Verwaltung eingenommen werden könne, würden dabei vor allem vor allem von der administrativen und politischen Spitze der Verwaltung vertreten, während das Ziel der Transparenz in zwei Ausführungen auftrete: als Transparenz der Verwaltung gegenüber der Bürgerin und der Öffentlichkeit und als Transparenz

[550] von Berg (1974, S. 73).
[551] von Berg (1974, S. 74).
[552] Grimmer (1974, S. 88).
[553] Grimmer (1974).
[554] Grimmer (1974, S. 88).
[555] Grimmer (1974, S. 90 f.).
[556] Grimmer (1974, S. 91).
[557] Grimmer (1974, S. 92).
[558] Grimmer (1974, S. 95).
[559] Grimmer (1974, S. 96). Dieses von Grimmer als „Trennprinzip“ (S. 97) bezeichnete Konzept findet sich später in der „informationellen Gewaltenteilung“ wieder.
[560] Rave (1974).

der Bürgerin gegenüber der Verwaltung, die auch von zwei unterschiedlichen Gruppen vertreten würden: denen, den es auch um die rechtsstaatliche Kontrolle der Verwaltung gehe, und denen, den es um die Kontrolle der Einzelnen gehe.[561] Vor dem Hintergrund der Befürchtungen einer Zentralisation der Macht beschäftigt sich Klaus Lenk mit den (De-)Zentralisations- und (De-)Konzentrationstendenzen der Verwaltungsautomation.[562] Unter Verweis auf die Verschwommenheit der in der Debatte präsentierten Vorstellungen versucht er sich an einer Klarstellung der verwendeten Begriffe und der dahinterstehenden Konzepte, die sich nicht auf die Aufbauorganisation der öffentlichen Verwaltung beschränke, sondern die Ablauforganisation in den Blick nehme, die weitgehend aus Entscheidungsprozessen bestehe: „Deren gründliche Analyse ist die unumgängliche Voraussetzung sowohl für die erfolgreiche Verwaltungsautomation wie für die Beurteilung der Konsequenzen der Informatik für die Struktur und die Funktionen der öffentlichen Verwaltung.“[563] Er unterscheidet dabei zwischen der „horizontalen funktionalen (De-)Zentralisierung“ und der „vertikalen funktionalen (De-)Zentralisierung“:[564] Erstere beschreibt die Zusammenfassung von Elementen, die mehreren Entscheidungsprozessen gemeinsam sind, letztere beschreibt die Abtrennung einzelner Elemente aus Entscheidungsprozessen und deren Zuordnung zu Organisationseinheiten auf einer anderen Ebene. Für Steinmüller besteht die Notwendigkeit der „Automatisierung der geistigen Arbeit“, „um die gestiegene und sonst unbewältigbare Komplexität der Gesellschaft beherrschbar zu halten.“[565] Er folgt seinem üblichen Vorgehen und beginnt mit der Darstellung der von ihm verwendeten Terminologie und seiner Grundannahmen: Datenschutz als „gesellschaftliche Informationskontrolle“ sei „die Menge aller Vorkehrungen zur Verhinderung unerwünschter Datenverarbeitung oder unerwünschter Folgen erwünschter Datenverarbeitung“, wobei unerwünscht sei, was „angebbaren – insbesondere rechtspolitischen – Zielvorstellungen widerspricht.“[566] Das Informationssystem sei ein Mensch-Maschine-System, dessen maschinelles Teilsystem als „Hilfssystem des Menschen“ aufzufassen sei, „das menschliche Informationsprozesse mit millionenfach größerer Schnelligkeit, Genauigkeit, Zuverlässigkeit und Komplexität ausführt und durch geeignete technische usw. Organisation im Stande ist, Ereignisse aus der Gesellschaft (im nicht erreichbaren Idealfall) in real-time aufzunehmen, zu verarbeiten und Anweisungen für eine adäquate Reaktion an den »Unternehmer« des Informationssystems zu geben.“[567] Mit der Informationsintegration entstünden „hochkomplexe Systeme neuer Art, deren wichtigste Eigenschaft es ist, informationelle Modelle über andere (reale oder ideelle) Systeme bereitzustellen und mit Hilfe dieser Modelle neue Informationen über die abgebildeten Systeme zu erzeugen.“[568] Anschließend beschreibt Steinmüller die bisherigen Lösungsansätze für das Problem der Informationskontrolle: So könne nicht die „Privat- oder Intimsphäre des einzelnen Staatsbürgers [...] das zu schützende Rechtsgut“ sein, denn diese Konzeption basiere auf der „überholten Gegenüberstellung von Individuum und Gesellschaft, Gesellschaft und Staat“, sei juristisch nicht bestimmbar und im Übrigen relativ „zum einzelnen Behörden- und Unternehmenszweck“.[569] Auch das Schutzgut „»personenbezogene Daten« als informationelle Abbildung der Privatsphäre“ sei untauglich: „Die Personenbezogenheit haftet Daten nicht als abstrakte

[561] Rave (1974, S. 121 ff.).
[562] Lenk (1974).
[563] Lenk (1974, S. 132).
[564] Lenk (1974, S. 130 f.).
[565] Steinmüller (1974, S. 187).
[566] Steinmüller (1974, S. 188 f.).
[567] Steinmüller (1974, S. 190).
[568] Steinmüller (1974, S. 191).
[569] Steinmüller (1974, S. 192 f.) unter Verweis auf die Abbildung eines spezifischen Teils des Rollenverhaltens von Individuen als Mittel zur Erfüllung spezifischer Funktionen.

Qualität an, sondern ergibt sich aus der jeweiligen Organisation eines Informationssystems“ und so könnten auch „Sachdaten, generelle und statistische Daten, selbst anonymisierte Daten zu personenbezogenen Daten verbunden werden.“[570] Auch würden beide vorgenannten Ansätze den Bedarf nach „informationelle[m] Minderheiten- und Institutionenschutz“ nicht erfüllen können.[571] Steinmüller hält es daher nicht für überraschend, dass „gegenüber diesem neuartigen Sachverhalt ein beliebtes Denkmuster juristischen Problemlösungsverhaltens versagt: Die »Verrechtlichungs« des gefahrbringenden Systems.“[572] Es reiche seiner Meinung nach nicht aus, „alle Informationsströme und -prozesse juristisch zu normieren, um die Gefahren zu bannen.“[573] Sein Gegenansatz gehe hingegen davon aus, dass „moderne Datenverarbeitung“ selbst die Mittel biete, ihre Gefahren zu steuern und die drei sich gegenüberstehenden widerstreitenden Interessen zu befriedigen: der Aufbau möglichst hochintegrierter Systeme, das Benutzerinneninteresse an Rationalisierung und Optimierung im Hinblick auf neu zu übernehmende Planungsaufgaben sowie das Interesse der Betroffenen, der Bürgerinnen, gesellschaftlicher Gruppen und Institutionen an „hinreichendem Schutz for informationeller Durchleuchtung und Verplanung.“[574] Es gehe um die *Organisation* von Informationsströmen derart, dass sie „funktionsspezifisch und kompetenzorientiert“ seien.[575] Dabei müsse „[d]ie Behördenstruktur mit ihrem je kompetenzspezifischen Informationsbedarf“ innerhalb des Informationssystems „durch eine entsprechende Daten- und Programmstruktur“ abgebildet werden, was juristisch die „Ausdehnung des Verfassungsgrundsatzes der Gesetzmäßigkeit der Verwaltung auf die Gesetzmäßigkeit der Informationsverarbeitung“ bedeute.[576] Zu erreichen sei das insbesondere durch strikte „Programmkontrolle“, denn „Software ist die objektivierte Problemlösungsstruktur, die zugleich die Informationskanäle regelt“,[577] aber auch durch „Abschottung“ als „Systemdifferenzierung zwecks Machtkontrolle“ zur Isolierung „besonders risikoreiche[r] Daten und Datenverarbeitung“.[578] Das alles gelte grundsätzlich auch für private Informationssysteme, deren Profitorientierung ein größeres Schutzbedürfnis und gleichzeitig eine geringere Kontrollfähigkeit nach sich ziehe.[579] Im Allgemeinen ungelöst sei das „Problem der Transparenz, die über Mensch-Maschine-Systeme künstlich hergestellt“ werden müsse, das als Aufgabe mithin an Kontrollinstitutionen übertragen und durch „Registrierungs- und Protokollpflichten“ unterstützt werden müsse.[580] Dann kommt Steinmüller zu einer verwegenen Schlussfolgerung:

> „Von Sondergebieten abgesehen kann heute die Datenschutzproblematik grundsätzlich als gelöst angesehen werden. Das Problem der Informationskontrolle in Staat

[570] Steinmüller (1974, S. 193). Siehe auch S. 205.
[571] Steinmüller (1974, S. 193 f.).
[572] Steinmüller (1974, S. 194).
[573] Steinmüller (1974, S. 195). Historisch ist genau das passiert: Der Gesetzgeber hat unter Verweis auf das Volkszählungsurteil den Datenschutz bereichsspezifisch umfassend gesetzlich geregelt.
[574] Steinmüller (1974, S. 195).
[575] Steinmüller (1974, S. 196).
[576] Steinmüller (1974, S. 196).
[577] Steinmüller (1974, S. 197).
[578] Steinmüller (1974, S. 199). Bezeichnend ist, dass Steimüller sowohl Abschottung als auch sensitive Daten hier schon in Anführungszeichen setzt. So wie der Personenbezug abhängig vom konkreten Informationssystem ist, ist auch Sensitivität keine Eigenschaft der Daten, sondern der Informationsverarbeitung. Explizit wird Steimüller letzteres erst später klarstellen.
[579] Steinmüller (1974, S. 200).
[580] Steinmüller (1974, S. 201). Den Kontrollinstitutionen schreibt Steinmüller darüber hinaus die „didaktische Aufgabe der Unterrichtung über anstehende Probleme und Lösungsmöglichkeiten“ zu.

> und Wirtschaft ist ungeachtet aller Teilprobleme prinzipiell und mit vertretbaren Mitteln lösbar.“[581]

Leider muss er dann konstatieren, dass der Kabinettsentwurf des Bundesdatenschutzgesetzes „unter dem Anschein umfassenden Datenschutzes ein äußerst durchdachtes System legislativer Durchbrechung vorsieht“,[582] das nicht anders verstanden werde könne, „denn als politische Absicherung der Automationsvorhaben des Bundes, der Länder und der Gemeinden vor dem öffentlichen Vorwurf mangelnden Schutzes des Bürgers und seiner Belange.“[583] Jochen Schneider versucht sich an den „Probleme[n] der Implementierung von »Privacy« in Informationszentren“.[584] Schutzobjekt des Datenschutzes sei der Mensch, allerdings würden die Regelungen des Datenschutzrechts kein Rechtsgut, „etwa die Privatsphäre“, bestimmen, „sondern stellen Bestimmungen für den Umgang mit Daten auf, um *dadurch* »Beeinträchtigungen schutzwürdiger Belange entgegenzuwirken«“.[585] Das zugrunde liegende Ziel sei demnach die Verhinderung von Missbrauch, „also de[m] unberechtigten Umgang mit Daten“[586] „Damit avancieren die Daten zum primären Schutzobjekt und entsprechend bleibt der Aspekt der Transparenz [der Person des Betroffenen] als übergreifendes Problem unberücksichtigt“, die auch bei berechtigtem Umgang entstehen könne.[587] Schneider möchte das Schutzgut „Privatsphäre“ aufrechterhalten, wenn auch nicht räumlich gedacht, sondern als „einer Kommunikation mit Vorbehalten (Westin) bzw. einem institutions- bzw. benutzerabhängigen Rollenspiel [(Müller)]“.[588] Auch will er „eine – trotz aller Relativität der Privatsphäre mögliche – grobe Bewertung der Daten nach Sensitivitäten“ vornehmen.[589] Im Gegensatz zu Steinmüller und Podlech hält Schneider einen Programmschutz für untauglich: „Je weniger aufgaben- und benutzerspezifisch aber ein Programm ist [...] desto geringer ist auch sein spezifischer Bezug zum »privacy« Problem [sic!]. [...] Insofern lassen nur aufgabenbezogene Programme eine solche Verrechtlichung zu.“[590] Albert Windolph, der kurz zuvor schon zusammen mit Helmut Rödl ein Auftragsgutachten zum Datenschutz für den Verband der Handelsauskunfteien, das vom bekannten – und inzwischen übernommenen – Inkassounternehmen Schimmelpfeng herausgegeben wurde, geschrieben hatte, war in seinem Beitrag einer der ersten, der das „in Artikel 5 GG verbriefte Recht auf Information, freie Meinungsbildung und Meinungsäusserung“ dem Datenschutz gegenüberstellte.[591] Darüber hinaus wendet sich Windolph explizit gegen die Einführung einer Gefährdungshaftung, wie sie noch im IPA-Entwurf zum Bundesdatenschutzgesetz „bei widerrechtlicher Speicherung, Einsicht, Änderung oder Vernichtung oder widerrechtliche[m] Abruf“[592] vorgesehen war und fordert eine Koordinierung bei

[581] Steinmüller (1974, S. 202).
[582] Steinmüller (1974, S. 202).
[583] Steinmüller (1974, S. 203). Er „belegt“ das durch „viele sonst rätselhafte Einzelbeobachtungen“: so etwa die Spezifika des gleichzeitig vorgelegten Entwurfs für ein Bundesmeldegesetz mit Personenkennzeichen, die „Einrichtung einer Informationspreisgabepflicht für alle Hochschulmitglieder im Bereich der Hochschule“, die „Umkehrung des Amtshilfeprinzips mit dem grundsätzlichen Verbot der Weitergabe von Daten zugunsten einer Weitergabepflicht“ oder der „Übergang von repressiver Kontrolle zu Prävention über polizeiliche und Kriminalinformationssysteme“ (heute: predictive policing).
[584] Schneider (1974).
[585] Schneider (1974, S. 207).
[586] Schneider (1974, S. 207).
[587] Schneider (1974, S. 207).
[588] Schneider (1974, S. 208). Zur Übernahme von Müllers Auffassung „von der Privatsphäre, die durch das Prinzip selektiver Informationsweitergabe qua Rolle [...] konstituiert wird“, siehe auch S. 209 f.
[589] Schneider (1974, S. 210).
[590] Schneider (1974, S. 212).
[591] Windolph (1974, S. 220).
[592] Windolph (1974, S. 217).

der Datenschutzgesetzgebung auf europäischer Ebene zur Verhinderung von Rechtsungleichheit und der daraus resultierenden Rechtsunsicherheit.[593]

Ulrich Dammann versucht 1974, das Datenschutzproblem und die bis dahin in der Diskussion vorgeschlagenen Lösungsstrategien vor dem Hintergrund des „Strukturwandels der Information“ und der „gesellschaftliche[n] Faktoren, Entwicklungsgesetzlichkeiten wie Interessenkonflikte“ einer eingehenden Analyse zu unterziehen.[594] Vor dem Hintergrund der bereits absehbaren Durchsetzung der Datenverarbeitung in allen gesellschaftlichen Teilbereichen unterscheidet er zwischen drei Dimensionen von mit der Informationsverarbeitung verbundenen Gefahren: einer „[e]xtensivere[n] und intensivere[n] »Verdatung«“ („mehr Sachverhalte“, „detailliertere Daten“), einer „[h]öhere[n] »Datenliquidität«“ („Datenträgeraustausch, Datennetze und integrierte Datenverarbeitung mit Fernzugriff“ mit einer „schnelleren und intensiveren Zirkulation der Daten“) sowie einer „[g]rößere[n] Angriffsfläche für Datenmißbrauch und Datenmanipulation“.[595] Für die gesellschaftliche Funktion des Datenschutzes bedeutet das nach Dammann:

> „Datenschutz kann sich weder darauf beschränken, die bestehende Informationsordnung zu konservieren und gegenüber den geschilderten Veränderungstendenzen zu immunisieren, noch darauf, durch flankierende Sicherheitsmaßnahmen einzelne offensichtliche Fehlleistungen oder Unglücksfälle auszuschließen. Datenschutz bedeutet vielmehr die Forderung nach einer humanen Steuerung des sich vollziehenden Veränderungsprozesses im Bereich der Information.“[596]

Die Auswirkungen dieser Veränderungen betrachtet Dammann getrennt nach Individuum und Gesellschaft.[597] Für das Individuum bedeuten sie die Gefahr von zunehmender Entfremdung – als Gegenstück zu einer Selbstdarstellung – und Festschreibung – im Sinne einer Aufhebung der Rollentrennung.[598] Die gesellschaftlichen Gefahren umfassen die Vereinfachung der sozialen Kontrolle und die Beschränkung der sozialen Mobilität – im Sinne der Deformation der politischen Meinungsbildung – sowie die Tendenz zur Monopolisierung des Wissens zugunsten von Organisationen einerseits und zugunsten von Führungsstrukturen andererseits.[599]

Anschließend analysiert Dammann grundsätzlich Einwände gegen das Konzept des Datenschutzes.[600] So werde vertreten, der Datenschutz diene entweder der Konfliktverschleierung: „Restriktive Informationshandhabung habe letztlich nur die Funktion, gesellschaftliche Konflikte, Vorurteile und nicht legitimierte Herrschaftsverhältnisse zu verdecken und damit zu konservieren.“[601] oder der Herrschaftssicherung: „Klassencharakter des Datenschutzes“ – „Datenschutz als Schutz der Privatsphäre nütze einseitig denjenigen, die sich Privatsphäre leisten können, sowie denjenigen, die diese brauchen, um öffentliche Kritik an ihren Privilegien gar nicht aufkommen

[593] Windolph (1974, S. 218).
[594] Dammann (1974b, S. 267).
[595] Dammann (1974b, S. 271). Eine Defnition des Begriffs „Datenmißbrauch“ fehlt dabei und auch aus der Beschreibung geht nicht hervor, ob es um den Datenumgang Unberechtigter oder um den unberechtigten Datenumgang grundsätzlich Berechtigter gehen soll, kurz: Es ist unklar, ob Datenmißbrauch als Teilaspekt von IT-Sicherheit oder von Datenschutz verstanden werden soll.
[596] Dammann (1974b, S. 274).
[597] Die „fruchtlos gebliebene Diskussion der Privatsphäre als Gefährdungs- und Schutzobjekt“ versucht Dammann, ähnlich wie Prosser (1960) fast 15 Jahre vorher, „zugunsten konkreter Kategorien zu überspringen.“ Dammann (1974b, S. 275, Fn. 6).
[598] Siehe Dammann (1974b, S. 275 ff.).
[599] Siehe Dammann (1974b, S. 278 ff.).
[600] Siehe Dammann (1974b, S. 280 ff.).
[601] Dammann (1974b, S. 280).

zu lassen."[602] Eine dritte Fundamentalkritik am Datenschutz ist – schon anfang der Siebziger – *post-privacy*:

> „Man selbst, so lautet üblicherweise die Argumentation, habe nichts zu verbergen; unbegrenzte Offenheit der Kommunikation sei nicht nur Voraussetzung für freie politische Willensbildung, sie entlaste auch von dem moralisch korrumpierenden Zwang zu partieller Unaufrichtigkeit, welche das von anderen als Rollenspiel apostrophierte Muster selektiver und differenzierter Informationsabgabe in Wahrheit darstelle."[603]

Diesen Kritikansätzen will Dammann auf drei Ebenen entgegentreten: auf der Ebene des abstrakten Datenschutzkonzepts, in Bezug auf „bestimmte Ausprägungen des Datenschutzes und deren Wechselwirkungen mit ihrem konkreten gesellschaftlichen Bezugsfeld" und auf der Ebene der konkreten Umsetzung, d. h. der Angemessenheit des Mittels.[604] Zwar sei die „konflikt*bestätigende* Wirkung" des Datenschutzes unbestreitbar, trage damit allerdings nicht notwendig zur Legitimation der Herrschaftsverhältnisse bei.[605] Den Vertreterinnen der „offenen Kommunikation" wirft er vor, damit „immer zugleich die von Konflikten befreite Gesellschaft" zu postulieren, denn das Datenschutzinteresse sei, so Dammann, das Produkt der „Existenz von Interessengegensätzen" – dem Modell der „offenen Kommunikation" fehle es also an „Realitätsbezug".[606] Auf der zweiten Ebene sieht Dammann die Frage des Klassencharakters des Datenschutzes angesiedelt, den er auch nicht verneint: „Datenschutz [...] ist ein Instrument der Interessendurchsetzung." Aber Datenschutz besitze auch „keine signifikante Affinität zu bestimmten gesellschaftspolitischen Zielvorstellungen", „entscheidend ist, wo, wie, für wen und für welchen Zweck Datenschutz eingesetzt wird."[607] Die zentrale Frage auf der dritten Ebene sei nach Dammann die „nach der Eignung des Datenschutzes als einer spezifischen Technik normativer Verhaltenssteuerung", vor allem im Hinblick auf den konkurrierenden Vorschlag einer Steuerung über Verwertungsverbote.[608] Wie schon die Hearings vor dem amerikanischen Kongress kommt auch Dammann zu dem Ergebnis, dass Verwertungsverbote nur eine geringe Steuerungswirkung haben.

Im Anschluss daran untersucht Dammann, von welchen „gesellschaftlichen Orten aus" welche Art von Datenschutzmaßnahmen mit welchen Erfolgsaussichten ausgehen könnten.[609] Das Individuum sei dabei in der schlechtesten Position, weil es „nur um den Preis seiner sozialen Entfaltung" den „Datenzwängen" entgehen könne.[610] Auch die Datenverarbeiter und die professionellen Entwicklerinnen könnten nur wenig zur Durchsetzung der Datenschutzziele beitragen, da der Datenschutz ihren Interessen zuwiderlaufe. Günstigere Aussichten für das Erkennen und Lösen von Datenschutzproblemen bestünden bei den „nicht unmittelbar ökonomisch orientier-

[602] Dammann (1974b, S. 280). Dass diese Annahme nicht völlig aus der Luft gegriffen ist, zeigt der Vorschlag, die Verbreitung von „bloßstellenden" Bildern zu pönalisieren, siehe etwa Mühlbauer (2014).
[603] Dammann (1974b, S. 281).
[604] Siehe Dammann (1974b, S. 281 ff.).
[605] Siehe Dammann (1974b, S. 281 f.). Gleichwohl gesteht Dammann ein, dass sich der Datenschutz als eine Strategie erweise, „die kurzfristig eher auf den befriedigenden modus vivendi *im* Konflikt als auf dessen aggressive Austragung gerichtet" sei (S. 282).
[606] Dammann (1974b, S. 282 f.). An diesem mangelnden Realitätsbezug hat sich bis heute nichts geändert.
[607] Dammann (1974b, S. 283).
[608] Siehe Dammann (1974b, S. 284).
[609] Siehe Dammann (1974b, S. 284 ff.).
[610] Siehe Dammann (1974b, S. 285). Die Mittel, die dem Individuum blieben, seien dabei nur Datenverweigerung und „Verschmutzung" der Datenkanäle, d. h. der Rückzug und die Abschottung. So später dann auch, allerdings aus positiv verkauft, Brunton und Nissenbaum (2011) unter dem Label „obfuscation".

ten Trägern bzw. Entwicklern“ von Informationssystemen.[611] Eine angemessene Lösung und Lösungsdurchsetzung könne jedoch nach Dammann nur auf der gesellschaftlichen Ebene angegangen werden: als gesetzliche Steuerung, als Marktsteuerung, durch öffentliche Nachfrage und öffentlichen Meinungsdruck.[612]

Abschließend betrachtet Dammann die rechtlichen Instrumente des Datenschutzrechts und unterscheidet „vier Typen von Datenschutz“ nach der Art und Weise, „wie auf den Informationsprozeß Einfluß genommen wird“: die Schutz von bestimmten Rechtsgütern, die Regulierung der Organisation der Datenverarbeiter, die Regulierung der Informationsprozesse selbst sowie sogenannte Verstärkungsregelungen.[613] Der erste Datenschutzansatz basiert auf der Beschreibung eines zu schützenden Rechtsgutes und/oder der Definition bestimmter verbotener Eingriffshandlungen.[614] Dammann sieht in der Diskussion zwei Rechtsgüter unterschieden: das Persönlichkeitsrecht und die Privatsphäre. Darüber hinaus nennt er – nach der Formulierung zu urteilen wahrscheinlich nur beispielhaft – drei Verletzungshandlungen: Informationsbeschaffung, Aufzeichnung und Weitergabe. Als eine Ausprägung sieht Dammann die Sphärentheorie, der er dann die bereits diskutierten Einwände entgegensetzt. Abschließend konstatiert er, dass erstens die „tradierte Dogmatik des allgemeinen Persönlichkeitsrechts“ von der Komplexität der Materie überfordert werde, zweitens „nach sozialen Bereichen differenzierende Regelungen“, wie sie auch Simitis gefordert habe, gebraucht würden und drittens „die Aufrechterhaltung und Stärkung der Steuerungskompetenz des Individuums“ von zentraler Bedeutung sei.[615] Der zweite Typ von Datenschutzrecht normiere die Organisation des Datenverarbeiters und beeinflusse dabei den Informationsprozess mittelbar.[616] Der dritte Ansatz reguliert die „Kommunikation selbst durch Erlauben, Gebieten und Verbieten von Informationshandlungen“ mit den Faktoren „Sender, Empfänger und Inhalt sowie ggf. Voraussetzungen, Zweck und Verwendung von Information“.[617] Nach Dammann gehörten etwa die Kontrollrechte der Betroffenen zu diesem Typus. Dieser Ansatz erlaube es darüber hinaus, „präzise Einzelregelungen schon vor einer Abklärung in der Rechtsgutdiskussion“ zu formulieren.[618] Den vierten Ansatz bezeichnet Dammann als Verstärkungsregelungen – Regelungen, die „(nur) der optimalen Durchsetzung anderweit vorgegebener materieller (Datenschutz-)Normen dient, ohne selbst materielle Festlegungen zu treffen“: Datensicherheitsvorschriften, Kontrollvorschriften sowie Schadensersatz- und Strafnormen.[619] Im Anschluss an diese Typisierung untersucht Dammann die rechtlichen Instrumente im einzelnen.[620]

[611] Siehe Dammann (1974b, S. 285). 40 Jahre später lässt sich konstatieren, dass Dammann mit dieser Aussage durchaus recht behalten hat, wenn er auch wohl nicht einberechnet hat, dass auch diese Akteurinnen Eigeninteressen vertreten, die sie nicht automatisch das Datenschutzproblem angemessen analysieren und „lösen“ lässt: Entwicklerinnen mit Eigeninteressen lösen in erster Linie die Probleme, an deren Lösung sie ein Interesse haben – das sind aber nicht unbedingt die Probleme aller (anderen) Betroffenen(gruppen).

[612] Siehe Dammann (1974b, S. 285 f.).

[613] Siehe Dammann (1974b, S. 286 ff.).

[614] Siehe Dammann (1974b, S. 287). Dieses Vorgehen sieht Dammann als typisch für das Strafrecht oder das zivilistische Deliktsrecht an.

[615] Siehe Dammann (1974b, S. 288).

[616] Siehe Dammann (1974b, S. 288). Vergleichbarkeit bzgl. Inhalt und Struktur sieht Dammann mit dem Presse- und sonstigen Medienrecht. In Podlech sieht er den profiliertesten Vertreter dieses Ansatzes, siehe Fn. 22.

[617] Siehe Dammann (1974b, S. 288).

[618] Siehe Dammann (1974b, S. 289). Diesen Ansatz sieht Dammann im Regierungsentwurf für ein Bundesdatenschutzgesetz verfolgt, siehe Fn. 23. Unklar bleibt allerdings, warum er hier nicht auf das Gutachten „Grundfragen des Datenschutzes“ verweist, obwohl er sonst umfangreichen Quellenangaben nicht abhold ist. Wahrscheinlich liegt der Grund darin, dass Dammann annimmt, dass es bei diesem Ansatz nur um materielles Datenschutzrecht gehe, wie aus seiner Analyse auf S. 290 f. abgeleitet werden kann.

[619] Siehe Dammann (1974b, S. 289).

[620] Siehe Dammann (1974b, S. 289 ff.).

Datensicherheitsvorschriften verfolgten das Ziel, „in tatsächlicher Hinsicht sicherzustellen, daß gesollte Informationsaktivitäten stattfinden können und nicht gewollte (Mißbrauch) verhindert werden“, ließen aber offen oder setzten voraus, „was befugt, also rechtmäßiger Gebrauch“ sei.[621] In Bezug auf die Regelung von Informationsprozessen betrachtet Dammann ausschließlich materiellrechtliche Regelungen und kritisiert die Forderung nach „vollständiger Normierung“, d. h. „Verrechtlichung“, im Sinne eines „detaillierte[n] und erschöpfende[n] materielle[n] Datenschutzrecht[s]“, die „ein[en] erhebliche[n] Teil bisher (rechtlich) freier gesellschaftlicher Kommunikation [...] austrocknen“ würde. Stattdessen müsse es bereichsspezifische Regelungen geben, wobei Dammann als Kriterien die Sensitivität der Daten, „die »Gefährlichkeit« [...] von Informationssystemen“, „technische und organisatorische Charakteristika der Informationsverarbeitung“ sowie die „Beziehungen zwischen Informationsverarbeitern und Betroffenen“ anlegen will.[622] Anschließend betrachtet Dammann die Rechte der Betroffenen auf Auskunft bzgl. der gespeicherten Daten, auf Auskunft bzgl. des Datenverkehrs, auf Korrektur und auf Löschung, die Pflichten der Datenverarbeiter zur Benachrichtigung und zu „periodischem Datenauszug“, die institutionellen Instrumente „Datenbank-Register“, „Steuerungs-/Überwachungsinstitution“ und Sanktionen sowie organisationsrechtliche Fragen wie das von Podlech vorgeschlagene Prinzip der Trennung von Betreiberinnen und Nutzerinnen von Informationssystemen.[623]

In einem der vom Hessischen Datenschutzbeauftragten Willi Birkelbach herausgegebenen „Beiträge zum Datenschutz“ versucht Hans-Joachim Reh, den Gegenstand und die Aufgabe des Datenschutzes zu analysieren und „einen neuen Ausgangspunkt für die Datenschutz-Diskussion zu finden“, wie Birkelbach im Vorwort vermerkt.[624] Reh kann Birkelbachs Wünsche in seinem Beitrag nicht erfüllen. Das liegt einerseits an der sehr zufällig wirkenden Zusammenstellung der von Reh betrachteten Aspekte, andererseits an Rehs Umgang mit den Quellen, die er in seiner Arbeit reproduziert: Er liefert Quellenangaben für Belanglosigkeiten, die er aber wörtlich zitiert, und präsentiert umfangreich Konzepte aus fremder Feder ohne Angabe ihrer Herkunft. Dem Datenschutz liegen seiner Meinung nach die „Interessengegensätze zwischen Individualinteresse auf der einen und Gemeinschafts-, Wirtschafts- oder anderen Gruppeninteressen auf der anderen Seite“ zugrunde und Informationsfreiheit und Datenschutz stünden „in einem Spannungsfeld“.[625] Das Ziel des Datenschutzes sei es, „den Mißbrauch einer durch Informationsspeicherung errungenen Machtposition auszuschließen, mindestens abzuwehren“, „Datenverarbeitungsanlagen und Informationssysteme“ durch Transparenz kontrollierbar zu machen und die Entstehung von Informationsmonopolen zu verhindern.[626] Als Individualrechtsschutz schütze der Datenschutz die Selbstbestimmung des Menschen als „wesentlichste Voraussetzung für eine Selbstverwirklichung in den Grenzen der Gemeinschaftsbezogenenheit und seiner Gemeinschaftsgebundenheit“ in erster Linie durch das Prinzip der Zweckbindung[627] und durch „Transparenz des Datenflusses“ und der Informationsverwendung.[628] Die zwei anderen von Reh angesprochenen Möglichkeiten eines Individualrechtsschutzes – über die Definition des Rechtsguts der Privatsphäre und

[621] Siehe Dammann (1974b, S. 289 f.). Daraus folgt, dass Sicherheitsmaßnahmen kein Selbstzweck sein können, auch wenn die Diskussion in der Informatik das im Hinblick auf die Vertraulichkeit – als Schutzziel der IT-Sicherheit – bis heute immer wieder behauptet.
[622] Siehe Dammann (1974b, S. 290 f.).
[623] Siehe Dammann (1974b, S. 291 ff.).
[624] Siehe Reh (1974).
[625] Siehe Reh (1974, S. 7).
[626] Siehe Reh (1974, S. 8).
[627] Siehe Reh (1974, S. 17). Der Abschnitt entbehrt jeder Quellenangabe.
[628] Siehe Reh (1974, S. 18). Auch dieser Abschnitt kommt ohne Quellenangabe aus.

die Sensitivität personenbezogener Daten – werden von ihm als untauglich abgelehnt.[629] Als gesellschaftspolitische Forderung beziehe sich der Datenschutz auf die Kontrolle von Informationsmacht, bei Reh vor allem im Sinne einer horizontalen und vertikalen Gewaltenteilung.[630] Dem Gesetzgeber rät Reh, einen „Fairness-Kodex“ aufzustellen, „der eine Generalklausel und einzelne Verfahrens- und Verhaltensregeln enthält, welche für alle Fälle der Datenverarbeitung Gültigkeit beanspruchen können.“[631] Die Generalklausel soll dabei lauten:

> „Das Sammeln, Speichern, Verarbeiten und Weitergeben von personenbezogenen Daten darf weder zur Entstehung von Informationsmonopolen führen, noch den Freiheitsraum des betroffenen Individuums stärker einschränken, als seine eigenen oder übergeordneten Interessen des Gemeinwohls es erfordern.“[632]

Die Verfahrens- und Verhaltensregeln, die Reh dieser Generalklausel beiseite stellen will und die er als „Datenverkehrs-Ordnung“ bezeichnet, sind eine etwas erweiterte Fassung der Fair Information Processing Principles, wie sie von der durch das Department of Health, Education and Welfare (HEW) eingesetzten Kommission vorgeschlagen wurden.[633]

Nachdem Podlech im ersten Beiheft der Datenverarbeitung im Recht (DVR) 1973 bereits den Datenschutz im Bereich der öffentlichen Verwaltung analysierte,[634] unternahm Bernt Bühnemann dies im Jahr darauf im vierten Beiheft der DVR für den nicht-öffentlichen Bereich.[635] Ziel seiner Untersuchung war es, den Entwurf der Bundesregierung für ein Bundesdatenschutzgesetz – vor allem im privaten Bereich – darauf hin zu überprüfen, ob das Bestimmtheitsgebot, das Gleichbehandlungsgebot sowie der Grundsatz der Verhältnismäßigkeit der Mittel eingehalten werden oder ob der Entwurf verfassungswidrig sei.[636] Im Ergebnis sowie in vielen Details lässt er kein gutes Haar an dem Entwurf. So erkläre das Gesetz in § 1, es sei sein Zweck, „personenbezogene Daten vor Mißbrauch bei der Datenverarbeitung zu schützen und dadurch der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken“, während das amtliche Vorblatt zum Gesetzentwurf aussage, es gehe um das „Recht[] des Schutzes der Privatsphäre vor Mißbräuchen bei der Datenverarbeitung“, aber auch um den Schutz „in allen schutzrelevanten Bereichen des öffentlichen und des privaten Lebens“ und um den Schutz „gegen die mißbräuchliche Verwendung der Daten“,[637] und die Begründung zu § 1 ausführe, „daß die Belange der Betroffenen das »primär« geschützte Rechtsgut seien, diese wegen der Relativität der Privatsphäre jedoch nicht unmittelbar, sondern nur auf dem Umweg über den Schutz der personenbezogenen Daten gewahrt werden können.“[638] Der zu verhindernde Missbrauch, der dem Gesetzentwurf auch seinen Titel gab: „Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung“, wird dabei, wie Bühnemann anmerkt, im Gesetz weder qualifiert noch –

[629] Siehe Reh (1974, S. 14 ff.). Quellenangaben gibt es hier nur für den Abschnitt zur Privatsphäre.
[630] Siehe Reh (1974, S. 18 ff.). Zwar spricht Reh auch die Informationsfreiheit an, behandelt sie dann aber ausschließlich als Problem des Parlaments, siehe S. 21 f. Die Quellenangaben in diesem Abschnitt sind haarsträubend: Einmal wird auf einen Text zum Insiderhandel verwiesen (Fn. 9), zum anderen auf einen Text zu den Informationsproblemen „des Verbandsabgeordneten“ (Fn. 10). Der Rest ist unbelegt.
[631] Siehe Reh (1974, S. 23).
[632] Reh (1974, S. 23).
[633] Siehe Reh (1974, S. 24 f.). Wenig überraschend zitiert Reh den Kommissionsreport U.S. Department of Health, Education, and Welfare (1973) nicht, dafür aber seinen Chef, Birkelbach, der die Einführung dieser Regelungen in einer Rede im August 1974 im Hessischen Landtag forderte.
[634] Siehe Podlech (1973a).
[635] Siehe Bühnemann (1974).
[636] Siehe Bühnemann (1974, S. 5).
[637] Siehe Bühnemann (1974, S. 3 f.).
[638] Siehe Bühnemann (1974, S. 30).

von einer Ausnahme abgesehen – überhaupt aufgegriffen.[639] Angesichts der Weite des Schutzes von natürlichen Personen in allen ihren Lebensbereichen hinterfragt Bühnemann darüber hinaus den Ausschluss von Personenvereinigungen und juristischen Personen aus dem Schutzbereich des Gesetzes, vor allem vor dem Hintergrund der Ausschlussbegründung, dass dieser Bereich gesetzgeberisch kaum fassbar sei und seine Einbeziehung die Praktikabilität beeinträchtigen würde.[640] Auch seien die schutzwürdigen Belange der Betroffenen, um deren Schutz es im Gesetz gehen soll, „nicht einmal [...] konstante Größen [...], da sie lediglich als Wertungspositionen in einen Wertungsprozeß einbezogen sind.“[641] Die Rechtslage führe zu einer Relativierung des Schutzes der Betroffenen und sei dabei noch schlechter als ein Rückgriff auf die von Lehre und Rechtsprechung entwickelten Fallgruppen zum allgemeinen Persönlichkeitsrecht, obwohl dieses auch unter dem Makel seiner Relativität leide.[642] Im Ergebnis hält Bühnemann fest, dass eine umfassende Regelung in der vorgelegten Art nicht erforderlich sei,[643] gegen Art. 5 GG verstoße, dem Bestimmtheitsgebot und dem Grundsatz der Verhältnismäßigkeit der Mittel widerspreche[644] und zieht das Fazit:

> „Gerade der vorliegende Entwurf bestätigt in aller Deutlichkeit, daß Begriffe wie Privatsphäre, schutzwürdige Belange der Betroffenen, personenbezogene Daten etc. allenfalls Orientierungshilfen bieten, für eine an rechtsstaatlichen Grundsätzen orientierte Gesetzgebung jedoch allein noch nicht ausreichen.“[645]

In einem vom Bundesministerium für Forschung und Technologie geförderten Forschungsbericht zum „Datenschutz“ veröffentlicht die Siemens AG, Bereich Datenverarbeitung, Vertriebsabteilung, „Mittel und Maßnahmen für die Datenverarbeitung“.[646] Mit dem Ziel angetreten, einen systematischen Überblick über juristische Aspekte und technische Maßnahmen des Datenschutzes zu geben, wird als Bedrohung die „Zusammenführung verschiedener Angaben aus den unterschiedlichen Lebensbereichen“ identifiziert, durch die „ein zu deutliches Bild des Einzelnen“ entstehen könne „(Transparenz)“, „sein Verhalten als Angehöriger von Gruppen wird prognostizierbar“ und bedrohe „[s]ein »Rollenverhalten« im Sinne freiheitlicher Selbstverwirklichung“.[647] Dem entgegen wollen die Verfasser alle „möglichen bzw. wirtschaftlich vertretbaren Vorkehrungen gegen unerwünschte, unberechtigte oder mißbräuchliche Verarbeitung personenbezogener Daten“[648] stellen, die „einen wirksamen und wirtschaftlich vertretbaren Erfolg ver-

[639] Siehe Bühnemann (1974, S. 101 f.).
[640] Siehe Bühnemann (1974, S. 24 ff.).
[641] Bühnemann (1974, S. 36).
[642] Siehe Bühnemann (1974, S. 36).
[643] Siehe Bühnemann (1974, S. 128 ff.).
[644] Siehe Bühnemann (1974, S. 144 ff.).
[645] Bühnemann (1974, S. 148).
[646] Amesberger et al. (1974). Als Verfasser werden Projektleiter Claus Amesberger, Klaus Eidmann, Peter Heder, Friedel Marksteiner und Jochen Schneider aufgeführt. Überschneidungen mit früheren Arbeiten Schneiders wie Schneider (1974) überraschen daher trotz dessen Position am Ende der Verfasserliste nicht.
[647] Siehe Amesberger et al. (1974, S. 7). Umfassend zu den rollentheoretischen Vorstellungen der Verfasser siehe S. 27. Der rollentheoretische Ansatz wird dabei als Erweiterung Westins „Kommunikation mit Vorbehalten“ verstanden. Er findet sich auch in den Schutzmaßnahmen wieder: In Erweiterung einer rollenbasierten Zugriffssicherung (RBAC) schlagen die Verfasser vor, auch die soziale Rolle der Betroffenen als Maßstab zu nutzen, „d. h. die Bestimmung der Zugriffsrechte unter Berücksichtigung der Rollen, die die Herausgabe der Daten bestimmt haben.“ (S. 69) Damit ließe sich etwa auch kontrollieren, ob es zu einer „»Anhäufung« von Ergebnissen nach Bereichen (Rollen) und in der Zeit“ komme (ebd.).
[648] Amesberger et al. (1974, S. 7).

sprechen“.[649] Obwohl der wirtschaftlichen Vertretbarkeit von Datenschutzmaßnahmen für den Datenverarbeiter ein durchgängig zu hohes Gewicht beigemessen wird und die Einzelmaßnahmen in technischer Hinsicht hoffnungslos veraltet sind, ist die Analyse der Interessenkonstellation fundiert und immer noch aktuell und die Schlussfolgerungen daraus für die Systemgestaltung immer noch angemessen:

> „Ganz offensichtlich soll der Datenschutz einen Ausgleich der Interessen zwischen Betroffenen (die durch die Daten in den Datenbanken beschrieben werden) und den Benutzern der Datenbanken bzw. der personenbezogenen Daten und den EDV-Anwendern schaffen. Aus den Interessenlagen resultieren unterschiedliche Anforderungen an ein Schutzsystem. Diese unterschiedlichen Anforderungen wiederum müßten gewichtet werden, um daraus Prioritäten für die Implementierung gewinnen zu können.“[650]

Während auf dem 48. DJT 1970 in Mainz nur eine relativ kleine Veranstaltung zum Thema Datenschutz stattfand, wurde unmittelbar vor dem 49. DJT 1972 eine Kommission unter der Leitung von Simitis[651] eingesetzt, die bis 1974[652] „Grundsätze für eine gesetzliche Regelung des Datenschutzes“ ausarbeiten sollte.[653] Die Thesen der Kommission wurden, wie im Vorwort deutlich gemacht wird, nicht von allen ihren Mitgliedern vertreten.[654] Es kann daher davon ausgegangen werden, dass Situationsbeschreibung und Problemanalyse eher der Summe der Ansichten der Beteiligten entsprechen, während die Forderungen eher auf dem Niveau des größten gemeinsamen Nenners bleiben. Obwohl das „Gutachten“ von der „[f]reie[n] Beschaffung, Verarbeitung und Verbreitung von Informationen“ als durch die Art. 2 I, 5 I und 20 I GG grundrechtlich geschützten Freiheiten ausgeht,[655] findet sich keine fundierte Auseinandersetzung mit den verfassungsrechtlichen Prüfungsmaßstäben Geeignetheit, Angemessenheit und Verhältnismäßigkeit im engeren Sinne. Stattdessen werden die Gefahren – Aufhebung der Privatsphäre, Beeinträchtigung in der Selbstbestimmung der sozialen Rolle des Individuums und Degradierung „zu einem steuerbaren Objekt derjenigen [...], die das Informationssystem kontrollieren“ – einfach postuliert.[656] Die Kommission fordert zu Regelung des Datenschutzes ein allgemeines Datenschutzgesetz sowie konkretisierende bereichsspezifische Vorschriften.[657] Das allgemeine Datenschutzgesetz solle dabei nur diejenigen „fundamentalen Bedingungen“ formulieren, „die für jede Informationsverarbeitung gelten“: Organisations- und Kontrollvorschriften, Rechte der Betroffenen und die Regelung

[649] Siehe Amesberger et al. (1974, S. 8). Die ganze Studie ist gefüllt mit Relativierungen rechtlicher Anforderungen, die etwa nur in ein „ausgewogenes Verhältnis“ zu den technischen Mittel zu bringen seien, wie es ebd. heißt.

[650] Siehe Amesberger et al. (1974, S. 60). „Benutzer“ sind dabei die Menschen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, während „Anwender“ Trägerinnen bzw. Betreiberinnen des Datenverarbeitungssystems sind.

[651] Andere aus der Datenschutzgeschichte bekannte Beteiligte waren Auernhammer, Bull, Kamlah, Kerkau, Podlech, Reh, Schmidt und Steinmüller als Kommissionsmitglieder sowie Dammann und Otto Mallmann.

[652] Das behauptet, wenn auch ohne Beleg, Bull in Bull (2009, S. 28). Andere Belege für diese zweijährige Arbeit der Kommission ließen sich nicht finden, jedoch wurde der Bericht zumindest 1974 veröffentlicht.

[653] Datenschutzkommission des Deutschen Juristentages (1974). Die Veröffentlichung enthält keinerlei Quellenangaben. Insofern lässt sich nur informiert raten, welcher der Beteiligten – die einzige Frau war die Sekretärin der Kommission – welche Idee einbrachte.

[654] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 6).

[655] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 11).

[656] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 11).

[657] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 20 ff.).

der Verarbeitungsphasen.[658] Die bereichsspezischen Regeln sollen dann auf der Basis einer Analyse der konkreten sozialen Situation und der daraus erwachsenden spezifischen Gefahren unter Berücksichtigung „[der] angewandten Verfahren, [der] Verarbeitungskapazität, [des] Umfang[s] der vorhandenen Angaben, [der] Organisationsform (integrierte und überregionale Systeme, Verbundmöglichkeit) sowie [des] Ziel[s] der Datenverarbeitung“ formuliert werden.[659] Es gebe nach Ansicht der Kommission weder „datenschutzirrelevante, freie Daten“ noch seien anonymisierte oder aggregierte Daten datenschutzirrelevant: Auch freie Daten seien „zu ganz bestimmten Zwecken mitgeteilt“ und dürften nicht zweckfremd verwendet werden, gerade dann nicht, wenn sie „um einer öffentlichen – vor allem auch politischen – Wirkung willen ganz bewußt in die Öffentlichkeit“ getragen worden seien.[660] Eine Minderheit der Kommission meint, vor diesem Hintergrund den Begriff der „personenbezogenen Daten“ allgemeingültig zu bestimmen und abgrenzen zu können:

> „Diese Begriffsbestimmung könne dahin gehen, daß personenbezogene Daten Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren (natürlichen) Person sind.[661] Damit sei auch die Problematik der Identifizierbarkeit von für statistische und andere Zwecke anonymisierten oder aggregierten Daten gelöst. Sobald und solange eine Person durch solche Daten bestimmbar ist, handle es sich eben um vom Gesetz geschützte personenbezogene Daten.“[662]

Im weiteren Gesetzgebungsverfahren nicht durchsetzen konnte sich die Kommission mit der Ausdehnung der Datenschutzkontrolle auf die Geheimdienste,[663] der Trennung von materieller öffentlicher Verwaltung und technischer Verwaltung[664] und der Genehmigungspflicht im nichtöffentlichen Bereich.[665] Auch die Annahme der Kommission über das sinnvolle Vorgehen bei der Gestaltung der Datensicherung: „Unter Berücksichtigung der in den Einzelsituationen zutage tretenden Risiken, sind die für den konkreten Fall erforderlichen Maßnahmen zu analysieren, vorhandene Methoden zu modifizieren oder auch neue zu entwickeln sowie die schließlich verwendeten zu einem spezifischen System der Datensicherung zusammenzufassen.“ und der daraus folgenden Schlussfolgerung, dass der Gesetzgeber sich „mit einer grundsätzlichen Regelung begnügen“ solle,[666] wurde nicht aufgegriffen. Zwar hat der Gesetzgeber keine Details der Datensicherung geregelt, aber eben auch nicht dafür gesorgt, dass die Datenverarbeiter aus fundierten situationsbezogenen Analysen ein konkretes, sinnvolles Schutzsystem ableiten müssen.

Selbst in der kurzen Hochphase der fundierten interdisziplinären Auseinandersetzung zum Datenschutzproblem in den siebziger Jahren nehmen die Jahre 1974 und 1975 eine Sonderstellung ein. Es waren die Jahre mit der höchsten Dichte interdisziplinärer Workshops, Kongresse

[658] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 22). Eine Minderheit in der Kommission fordert sogar, in das allgemeine Datenschutzgesetz „nur rein formelle Regeln aufzunehmen“ und das materielle Datenschutzrecht ausschließlich in bereichsspezifischen Gesetzen zu regeln, ebd.

[659] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 25).

[660] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 26 ff.).

[661] Diese Minderheit hat sich durchgesetzt, wie ein Blick auf § 3 Abs. 1 BDSG zeigt: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“ Die in der Kommission diskutierte Erweiterung des Datenschutzrechts auf Personengruppen und juristische Personen, die zumindest in einen Prüfbeschluss mündete, siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 30), wurde allerdings nie umgesetzt.

[662] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 28).

[663] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 34 f.).

[664] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 36).

[665] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 38 f.).

[666] Siehe Datenschutzkommission des Deutschen Juristentages (1974, S. 51).

und Symposien, deren Ergebnisse dann im Laufe der folgenden Jahre dokumentiert wurden. Aus den Problembeschreibungsansätzen und Lösungsideen waren vollständige Erklärungsmodelle und umfassende und konsistente Lösungskonzepte geworden, deren Ecken und Kanten in den vorangegangenen Diskussionen abgeschliffen worden waren und die bereits den Test der kritischen Begutachtung durch die wissenschaftliche Gemeinschaft bestanden hatten. Gleichzeitig war die Diskussion noch nicht hinabgestiegen in die detailverliebte Auseinandersetzung um einzelne Formulierungen in Gesetzestexten und deren Auslegung.

Die Zeitschrift Bild der Wissenschaft lud im März 1974 zu einem Streitgespräch über den Gesetzentwurf der Bundesregierung zum Datenschutz und die diesem zugrunde liegenden und durch dieses zu regelnden Gefährdungen, dessen Ergebnisse im Jahr darauf in einem Band veröffentlicht wurden.[667] In seiner Einleitung verweist Helmut Krauch darauf, dass der Gesetzentwurf „in erster Linie das Ziel [verfolgt], die Privatsphäre des Bürgers zu schützen“[668] – ein Ziel, das er dann gleichsetzt mit dem „Freiheitsrecht der Selbstdarstellung“,[669] nur um dann die inhaltlich wohl breitestmögliche Beschreibung des Datenschutzproblems zu liefern:

> „Wichtigstes Problem ist es daher, Kontrolle über den Machtzuwachs auszuüben, der durch Datenbanken und Informationssysteme entsteht. Dabei geht es keineswegs allein um den Schutz der Individualsphäre des einzelnen Bürgers, sondern um die Gefahr einer gegen die Verfassung verstoßenden Machtausübung. Wer über große Mengen von Daten über das Verhalten von Gruppen oder einer ganzen Bevölkerung verfügt, wer Informationen hat über die Wandlung politischer Einstellungen, über Sozialisationsprozesse, über den Zusammenhang zwischen Psyche und politischem Verhalten und wer aus diesen Daten psychometrische und soziometrische Simulationsmodelle aufstellen und auswerten kann, der ist auch in der Lage, politische Alternativen in bezug auf ihre Durchsetzbarkeit, insbesondere auch gegen wesentliche Interessen von einzelnen Bürgern, abzuschätzen. Dadurch entstehen für die Verwaltung Dispositionsvorteile und Manipulationsmöglichkeiten, wie sie von der Wirtschaft im Rahmen der modernen Marketingmethoden bereits angewandt werden. Wenn es in Zukunft auch noch zu einer systematischen Kombination von Verwaltungsdaten und Simulationen und marktorientierter Disposition kommt, so bedeutet das für die meisten einzelnen Bürger einen ungeheuren Machtverlust.“[670]

Im ersten Beitrag präsentiert der Hessische Landesdatenschutzbeauftragte Willi Birkelbach seine „Überlegungen nach dreijähriger Datenschutzpraxis“.[671] Für ihn geht es um die Bedrohung der „freie[n] und unkontrollierte[n] Entfaltungsmöglichkeit des Menschen durch Einblicke in seine Privatsphäre und durch die Möglichkeit der Manipulation mit den so gewonnenen Informationen“ durch integrierte Informationssysteme und unkontrollierte Datenflüsse.[672] Dem will Bir-

[667] Siehe Krauch (1975b). Die Teilnehmerinnen werden in der Einleitung als „Rechtswissenschaftler, Verwaltungs- und Wirtschaftsexperten sowie Zukunftsforscher“ bezeichnet, siehe Krauch (1975a, S. 7). Es bleibt leider unklar, wer genau zu diesem Streitgespräch eingeladen wurde, denn den zu Aufsätzen ausgearbeiteten Diskussionsbeiträgen wurden weitere Aufsätze aus den Disziplinen Rechtswissenschaft, Psychologie und Soziologie zur Seite gestellt, siehe Krauch (1975b, S. 9).

[668] Krauch (1975a, S. 7).

[669] Krauch (1975a, S. 8).

[670] Krauch (1975a, S. 8). Im Grunde heißt diese Darstellung der drei einander wenn nicht ausschließenden, jedenfalls aber sich nur wenig überschneidenden Begründungszusammenhänge für das Datenschutzgesetz, dass Krauch nicht in der Lage ist, sich entweder für eines der drei Schutzgüter zu entscheiden oder sie tatsächlich als *ein* Schutzgut darzustellen.

[671] Siehe Birkelbach (1975).

[672] Siehe Birkelbach (1975, S. 11 f.).

kelbach einen „Fairneßkodex“ entgegenstellen, „der eine Art Konsensus dessen darstellt, was in einer freien demokratischen Gesellschaft unter fairem Umgang mit Informationen zu verstehen ist, und der für alle Arten der Informationsverarbeitung gilt“[673] und aus dem heraus dann ein Datenschutzgesetz zu entwickeln sei. Die Entwicklung des Datenschutzgesetzes habe dabei schrittweise zu erfolgen: Ausgehend von allgemeinen Regel – „daß Daten nicht in einer das Persönlichkeitsrecht gefährdenden Weise verwendet werden dürfen“ – müssen diese „im Laufe der Zeit und aufgrund der in der Datenschutzpraxis gemachten Erfahrungen“ ergänzt werden durch bereichsspezifische Regelungen.[674] Auch Seidel sieht im dritten Beitrag die Datenverarbeitung als Bedrohung für eine Privatsphäre, distanziert sich allerdings von der Sphärentheorie, da sie kategorisch zwischen Öffentlichkeits- und Privatsphäre unterscheide, während Seidel aus einer weit vorangeschrittenen Verzahnung des privaten und öffentlichen Lebens schlussfolgert, dass das Persönlichkeitsrecht gerade auch in seinem öffentlichen Ausleben geschützt werden müsse.[675] Trotz allem will Seidel aber am Schutzgut der Privatsphäre im Sinne eines zurückgezogenen Privatlebens festhalten, das zu schützen sei vor dem Zwang eines Sich-öffnenmüssens.[676] Das ungestörte Privatleben, die Individualität des Menschen, die Geheimsphäre, das Recht des Menschen auf Intransparenz und die Persönlichkeitssphäre sind auch für Auernhammer die Schutzgüter des Datenschutzrechts,[677] der anschließend begründet, warum der Entwurf für ein Bundesdatenschutzgesetz dem einzig angemessenen Weg eines Mittelwegs zwischen der umfassenden Kodifizierung des Datenschutzsrechts und allein bereichsspezifischen Ergänzungen bestehender Rechtsnormen folgt und als Auffanggesetz ausgestaltet ist.[678] Podlech stellt der Privatsphärenschutzsicht zwei durchaus andere Problemaspekte gegenüber: „[D]ie Herstellung von Persönlichkeitsprofilen und die Verdinglichung der sozialrelevanten Informationen einer Person in die Warenform [...] widerspricht dem unter dem Topos »Persönlichkeitsrecht« durch Artikel 2 Abs. 1 des Grundgesetzes gewährleisteten Recht auf Erhaltung der Selbstdarstellungsmöglichkeit der Bürger“, wobei Selbstdarstellung dabei „der empirisch beschreibbare soziale Interaktionsvorgang [heißen soll], in dem Menschen selbstbewußte Individualität gewinnen.“[679] Karhausen erklärt die rollenspezifische Exklusivität der Informationspreisgabe zum Schutzgut des Datenschutzes und definiert daher „Mißbrauch“ als Bruch der „akzeptierten und beabsichtigten Verwendungsregeln“.[680] Klaus Lenk benutzt zwar den Begriff der Privatsphäre, allerdings nur als „Symbol“ für die „Ohnmacht gegenüber allwissenden Institutionen“, die „Manipulationen der Medien, um Nachrichten zu kontrollieren und Meinungen zu formen“, die „Reduzierung von Menschen auf Nummern“ oder auch den Konformitätsdruck:[681] „[D]urch neue Informationstechnologien [wächst] die Transparenz des menschlichen Verhaltens, seine Sichtbarkeit, leichte Beobachtbarkeit [...]. Unmittelbar folgt daraus, daß Überwachung als ein Mittel sozialer Kon-

[673] Birkelbach (1975, S. 14). Der Autor hat in seiner Ausarbeitung fast keine seiner Informationsquellen angegeben, es ist daher auch nicht wirklich überraschend, dass er hier nicht angibt, aus welcher Quelle er diesen Vorschlag übernimmt.

[674] Siehe Birkelbach (1975, S. 19 f.).

[675] Siehe Seidel (1975, S. 38 f.).

[676] Siehe Seidel (1975, S. 46 f.).

[677] Siehe Auernhammer (1975, S. 57). Siehe auch S. 64 f., wonach es beim Bundesdatenschutzgesetz tatsächlich ausschließlich darum gehen soll, die Privatsphäre des Individuums zu schützen. Der Weg über die personenbezogenen Daten sei nur deshalb notwendig, weil anders dieser Schutz nicht sichergestellt werden könne, auch wenn damit Daten umfasst würden, die die Privatsphäre nicht berührten.

[678] Siehe Auernhammer (1975, S. 60 f.).

[679] Podlech (1975b, S. 73).

[680] Siehe Karhausen (1975, S. 83). Die Übereinstimmung Schoemans Ziel eines Schutzes der „spheres of life“ (1992) sowie Nissenbaums „contextual integrity“ (2004) mit diesem Konzept ist unübersehbar.

[681] Siehe Lenk (1975, S. 95).

trolle dichter wird, gleichviel ob dies von (Teilen) der Gesellschaft gewünscht wird oder nicht“,[682] so Lenk unter Verweis auf die Rollentheorie. Beschränkungen der Sichtbarkeit und der Transparenz menschlichen Verhaltens dienten auf der individuellen Ebene dem Schutz der persönlichen Autonomie vor möglicher Diskriminierung durch informationell Mächtigere, darüber hinaus seien sie „für den Bestand der Gesellschaft und für das Funktionieren der Mechanismen der sozialen Kontrolle unerläßlich“ und dienten drittens der Beschränkung politischer Macht.[683] Um die Ebene der politischen Macht geht es auch Dammann bei der Untersuchung von Planungsinformationssystemen auf die Möglichkeiten der von der Planung Betroffenen, ihre Interessen in den Planungsprozess – und damit in die Planungsentscheidung – einbringen zu können, auch damit „die kontroversen Auffassungen über Situationen, Probleme und Zielvorstellungen“ ausgehandelt werden können.[684] Entscheidungs- und Planungsinformationssysteme vergrößerten die Handlungsmacht des planenden Subjekts gegenüber allen anderen gesellschaftlichen Kräften und entzögen der demokratischen Öffentlichkeit, aber auch den Parlamenten, mehr und mehr die Kontrolle über den Planungsprozess.[685] Einerseits würde damit die demokratische Legitimation von Planungsentscheidungen durch die „Rationalität des technischen Vorgangs“ ersetzt, obwohl weder Daten, Fragestellungen oder Erhebungsmethoden noch Darstellungs- und Analyseverfahren objektiv seien, sondern immer interessengebunden. Andererseits bestehe die Gefahr, dass Planungsinformationssysteme dazu genutzt würden, „die Macht der etablierten Kräfte zu vergrößern und das demokratische Prinzip des Machtwechsels auszuschalten.“[686] Um diese Probleme abzuwenden, reiche es nicht, die Planungsdaten offenzulegen – heute als „open data“ bekannt –, sondern es müssten auch die Prämissen der Modellrechnungen offengelegt werden im Sinne eines „open model“.[687] Auch Müller versucht, die soziologische Rollentheorie als Erklärungsmodell für das Datenschutzproblem zu nutzen: Die „verschiedenen Rollenverpflichtungen bestimmen unsere Informationsweitergabe *gegenüber* Institutionen. Aber unsere Rollen bestimmen nur begrenzt die Datenweitergabe *zwischen* Institutionen.“[688] Dadurch ändere sich jedoch das Institutionengeflecht für das Individuum, aber auch für andere soziale Akteure: Vormals getrennte, weil funktional differenzierte, Institutionen veränderten sich zu einer „kommunikativen Einheit“:[689] „Vordergründig erscheint dies nur als eine Effizienzerhöhung, als eine Komplexitätsreduzierung für Institutionen, sie ist aber gleichbedeutend mit einer Komplexitätssteigerung dieses Institutionengeflechts für den Bürger.“[690]

Unter dem Titel „Der numerierte Bürger und die Informationsgesellschaft“ trafen sich im November des gleichen Jahres vierundzwanzig Wissenschaftlerinnen und Praktikerinnen aus dreizehn Disziplinen im Zentrum für interdisziplinäre Forschung an der Universität Bielefeld zu einem Kolloquium, das nach der im Juni vom PEN-Zentrum Bundesrepublik Deutschland verabschiedeten Resolution zum Datenschutz organisiert worden war. Der kurz darauf – und damit vor der Dokumentation der Erfassungsschutz-Veranstaltung – erschienene Tagungsband enthält sowohl die Beiträge als auch einen großen Teil der Diskussionen zu den Beiträgen.[691]

[682] Lenk (1975, S. 99 f.).
[683] Siehe Lenk (1975, S. 101 f.).
[684] Siehe Dammann (1975, S. 107).
[685] Siehe Dammann (1975, S. 110 ff.).
[686] Siehe Dammann (1975, S. 112).
[687] Siehe Dammann (1975, S. 116 f.).
[688] Müller (1975c, S. 141).
[689] Siehe Müller (1975c, S. 145). Müller beschreibt das nur für die öffentliche Verwaltung, aber es hat auch für den privatwirtschaftlichen Bereich Geltung.
[690] Müller (1975c, S. 145).
[691] Siehe Hoffmann et al. (1975, S. 7 f.).

Wilhelm Opfermann, Assistenzprofessor im Fachbereich Rechtswissenschaft der Freien Universität Berlin, versucht, zwei Kategorien von Informationsansprüchen der Bürgerin zu trennen: Betroffenheitsansprüche – auf Informationen, die sich auf die Bürgerin selbst beziehen, – und Informationsteilhabeansprüche – auf Informationen, die sie in ihrer Rolle als Bürgerin interessieren. Für die Informationsteilhabeansprüche untersucht er dann, ob sie als zwingender Anspruch aus dem Grundrecht auf Informationsfreiheit abgeleitet werden können und verneint das. Abschnließend verneint er auch die Wünschbarkeit eines individuellen Teilhaberechts und verweist stattdessen auf die Möglichkeit, die individuelle Teilhabe durch politische und wirtschaftliche Organisationen vermitteln zu lassen.[692] Letzteres wird in der Diskussion vor dem Hintergrund der asymmetrischen Machtverteilung in Organisationen zwischen der Leitung und den Mitgliedern stark kritisiert.[693] Podlech geht in seinem Beitrag explizit von der liberalen Konzeption des Individualschutzes aus und benennt als Regelungsziele, „daß erstens die den Privatmenschen (bourgeois) in seiner Freiheit schützende Grundrechtsgewährleistung am besten zugleich den politisch engagierten Bürger (citoyen) in seinen politischen Freiheitsräumen schützt“.[694] Das Persönlichkeitsrecht als „Recht auf Erhaltung der Selbstdarstellungsmöglichkeit“ der Bürgerin werde durch die Bildung von – Zeit und Sektorengrenzen überwindenden – Persönlichkeitsprofilen und die Verwarenförmigung der sozial relevanten Informationen einer Person bedroht.[695] In der Umsetzung unterscheidet er materiellen von organisatorischem Datenschutz. Ersterer sei das Auswahlprinzip, „das aus der Menge technisch möglicher Informationsvorgänge die Menge sozial verträglicher“ auswähle, letztere würden „durch Einführung besonderer Organisations- und Verfahrensformen die Einhaltung der materiellen Datenschutzvorschriften bis auf einen sozial tragbaren Rest erzwingen“.[696] Erst nach der Diskussion problematisierte Podlech, dass in der bisherigen Datenschutzdiskussion „die Gefährdungen individueller Freiheitsräume durch das Informationsverhalten gesellschaftlicher Großverbände oder Institutionen wie *Kirchen*, *Gewerkschaften*, *Unternehmensverbände* und *Presse*“ nahezu unberücksichtigt geblieben sei.[697] Barbara Tietze kritisiert in der Diskussion Podlechs Analyse der kompensatorischen Funktion von Familie und Wohnung und insbesondere, dass er vertrete, deren Schutz aufrechtzuerhalten. Stattdessen müsse das Problem von der anderen Seite angegangen werden: Die „Selbstdarstellung des Individuums und die selbstbewußte Individualität in den Bereichen der Öffentlichkeit, das ist der Bereich politischer Partizipation und der Bereich der Organisation von Arbeit“, müssten garantiert werden, dann werde „auch diese kompensatorische Funktion von Familie und Ehe relativ unwichtig“.[698] Eggert Schwan erläutert in seinem Beitrag, dass er es zwar rechtspolitisch für relevant halte, wie Walter Schmidt die allen Freiheitsrechten zugrunde liegende Entscheidungsfreiheit zum Diskussionsgegenstand zu machen, rechtsdogmatisch müssten diese verschiedenen Freiheitsbereiche aber voneinander unterschieden werden, und begründet damit auch, warum die

[692] Siehe Opfermann (1975).
[693] Siehe Hoffmann et al. (1975, S. 26).
[694] Siehe Podlech (1975a, S. 27).
[695] Siehe Podlech (1975a, S. 29). Vorstellungen Goffmans von *privacy* aufgreifend beschreibt er dann die Grundrechte auf Schutz von Ehe und Familie und auf Unverletzlichkeit der Wohnung in ihren informationellen Dimensionen als Schutz des sozialen und des räumlichen Ortes „problementlasteten Rollenwechsels unabhängig von der sozialen und architektonischen Struktur dieses Ortes“, ebd.
[696] Siehe Podlech (1975a, S. 30 f.).
[697] Siehe Podlech (1975a, S. 32).
[698] Siehe Hoffmann et al. (1975, S. 35). Es handelt sich um eine Argumentation, die viel später teilweise von den Vertreterinnen einer *post-privacy* wieder aufgegriffen wurde und dort – verkürzt – heißt: Die kompensatorische Funktion von Privatsphäre sei überflüssig, weil sich ja alle in ihrer selbstwussten Individualität in der Öffentlichkeit ausleben könnten, siehe dazu etwa Heller (2011).

zu Art. 2 Abs. 1 entwickelte Sphärentheorie grundsätzlich zu Analyse staatlicher Informationssammlung nicht anwendbar sei.[699] In der Diskussion ergänzt Steinmüller, dass das BVerfG „zwar mehrfach von einem angeblich »unantastbaren Kernbereich privater Lebensgestaltung«“ gesprochen habe, sich aber nicht imstande gesehen habe, „ihn zu benennen.“[700] Kerstin Anér berichtet vom schwedischen Ansatz, eine (Multi-Stakeholder-)Kommission – die „Dateninspektion“ – einzusetzen, deren Aufgabe es sei zu verhindern, dass „die Privatsphäre“ durch „Personenregister“ oder „Datenregister“ verletzt werde, ohne dass das Gesetz „Privatsphäre“ definiert habe. Basierend auf einem Genehmigungsmodell für Datenbanken entscheidet die Kommission fallweise, wobei eine Verkettung zwischen zwei „Registern“ als eigenes „Register“ betrachtet und damit selbst wieder genehmigungspflichtig ist.[701] Aus schwedischer Sicht gebe es daher auch keinen Widerspruch zum Schwedischen Transparenzgesetz von 1766, im Gegenteil: Je weniger „Register“ es gebe, desto leichter ließe sich kontrollieren, wer darauf zugreife. Es dürfe also „keine größere Menge allgemeiner Personenregister über alle Schweden geben.“[702] Im Zusammenhang mit seiner Analyse der „Machtverteilung zwischen Parlament und Verwaltung in der Informationsgesellschaft am Beispiel der USA“ legt Hans D. Jarass offen, von welchen Grundannahmen und -bedingungen der sozialen Informationsverarbeitung die erste Generation der Datenschützerinnen ausging.[703] In allen Phasen der Informationsverarbeitung werden Entscheidungen – auch Wertentscheidungen, aber nicht nur solche – getroffen, deren Konsequenzen eine notwendige Einseitigkeit der Informationen sind, die gleichzeitig gegenüber möglichen Nutzerinnen tendenziell verborgen bleiben: Alle Informationssysteme sind zweckorientiert, und die Zwecke werden von sozialen Akteurinnen gesetzt. Informationssysteme sind daher immer auf die Bedürfnisse der Zwecksetzerinnen zugeschnitten.[704] In der anschließenden Diskussion fordert Dammann, dass es eine „ausreichende Modellflexibilität und den notwendigen Modellpluralismus“ geben müsse.[705] Elisabeth Endres analysiert – vorwiegend für staatliche Datenbanken – das Zusammenspiel von „Datenerfassung“ und „Datenzugang“.[706] Für die Datenerfassung stellt sie fest, dass diese – unter den Bedingungen der Ausweitung der Staatsaufgaben in der modernen Gesellschaft – umfassend notwendig sei, sie aber „zumindest in ihren negativen Auswirkungen“ einzuschränken sei. Es werde „Geheimhaltung gefordert, Persönlichkeitsschutz, eventuelle Löschung, mitunter soll auch ein Bereich aus der Erfassung ausgeklammert werden. Der Effekt derartiger Postulate darf nicht unterschätzt werden.“[707] Die wesentliche Gefahr sei dabei allerdings nicht „die Gefahr der Indiskretionen, also des Verrats geschützter Daten an unbefugte Personen“, sondern die Gefahr der Überwachung, vor allem der politischen Überwachung, von Individuen und Gruppen.[708] Als Lösung schlägt Endres eine doppelte Demokratisierung vor: „einmal Demokratisierung der Erfassungskriterien, dann Demokratisierung des Zugangs.“[709] Die Demokratisierung der Erfassungskriterien habe nach Endres drei Voraussetzungen: Erstens müsse die Sprache des Sachgebietes allgemeinverständlicher werden, zweitens sei der Zweck anzugeben und drittens müsse zu den geplanten Erfassungskriterien eine „objektive[] Beurteilung“ mitgeliefert werden, „was

[699] Siehe Schwan (1975b).
[700] Siehe Hoffmann et al. (1975, S. 41).
[701] Siehe Anér (1975).
[702] Siehe Anér (1975, S. 46).
[703] Siehe Jarass (1975), vor allem die S. 56 ff.
[704] Siehe Jarass (1975, S. 56 ff.).
[705] Siehe Hoffmann et al. (1975, S. 61).
[706] Siehe Endres (1975).
[707] Endres (1975, S. 64).
[708] Siehe Endres (1975, S. 64).
[709] Siehe Endres (1975, S. 66).

sich mit dergleichen Speicherungen kontrollieren und vorausplanen läßt.“[710] Steffen Harbordt untersucht Entscheidungs- und Planungsprozesse in der öffentlichen Verwaltung, die unter der Verwendung von Computersimulationen ablaufen, auf ihre Gefahren für die Beteiligungsmöglichkeiten sowohl des Parlaments wie auch der Bürgerinnen.[711] Dabei verweist er insbesondere darauf, dass die Simulationen und die dabei gewonnenen Ergebnisse – „die zweckmäßigste Entscheidung“, Mittel-Zweck-Relationen, Auswirkungen und Nebenwirkungen oder Alternativen[712] – von Nichtfachleuten nicht kontrolliert werden könnten, weil ihnen das erforderliche Spezialwissen fehle und sie damit die den Simulationen zugrunde liegenden Modellannahmen und Daten-, Variablen- und Parameterauswahlentscheidungen nicht hinterfragen könnten.[713] Stattdessen würde es gesellschaftlich bereits dominierenden Interessengruppen leichter fallen, ihre Interessen vermittels solcher Simulationen – und den diesen eigenen Wahrheitsunterstellungen – durchzusetzen:

> „Sie prägen die Sichtweise, mit der ein bestimmter Problembereich gesehen und in einem Modell abgebildet wird. Davon hängt ab, welche Variablen und Beziehungen als wesentlich in das Modell aufgenommen werden und welche vernachlässigt werden. Die dominierenden Interessen können ferner die Anlage der Modellexperimente beeinflussen, nämlich, nach welchen Kriterien eine Lösung als »optimal« definiert wird, welche Maßnahmen überhaupt auf ihre Konsequenzen untersucht und welche von vornherein ausgeschlossen werden, welche Größen als veränderbar angesehen werden und welche als vermeintliche Konstanten gelten [...]. Dementsprechend besteht eine sehr hohe Wahrscheinlichkeit, daß auch die Entscheidungsvorschläge von diesen Interessen geprägt sind.“[714]

Mit Verweis auf Dammanns Identifizierung der Information als einem „immer wichtiger werdenden Rohstoff und sozialen Machtfaktor“ schlussfolgert Harbordt, dass die Verteilung der Machtfaktoren Information und Informationsverarbeitungskapazität der „ungleichen Verteilung wirtschaftlicher und politischer Macht“ entsprechen und die Ungleichheit zwischen den mächtigen Gruppen und den Ohnmächtigen noch verstärken werde.[715] Müller präsentiert ausführlich sein „Privatsphären“-Modell, das auf einem modifizierten rollentheoretischen Ansatz basiert, zusammen mit den Ergebnissen der Auswertung einer empirischen Studie zur Datenweitergabe zwischen Institutionen.[716] „Privatsphäre“ bedeute nach Müller aus der Sicht des einzelnen die „Aufrechterhaltung der unterschiedlichen Bilder, die über ihn bei anderen Personen oder Institutionen existieren“ und sei das Ergebnis sozialer Interaktionen in modernen, hochdifferenzierten Gesellschaften, mit denen die sozialen Verpflichtungen generell aufrechterhalten, aber einige nur minimal abgesättigt würden. Diese rollenspezifische oder selektive Informationsweitergabe ermögliche die unterschiedliche – und voneinander unabhängige – Erfüllung sozialer Verpflichtungen, von Rollenerwartungen, und erzeuge „kontrolliertes Nichtwissen über Dinge, die jeweils

[710] Siehe Endres (1975, S. 66 f.).
[711] Siehe Harbordt (1975).
[712] Siehe Harbordt (1975, S. 71).
[713] Siehe Harbordt (1975, S. 72 ff.).
[714] Harbordt (1975, S. 76).
[715] Siehe Harbordt (1975, S. 77). Zumindest die Bezeichnung der Information als Rohstoff, mehr noch, als dem „vielleicht bedeutendsten Rohstoff“, ist älter und wurde auch schon von Hans-Dietrich Genscher, der bis Anfang 1974 Bundesinnenminister war, gebraucht, siehe Hoffmann et al. (1975, S. 173).
[716] Siehe Müller (1975a). Müller hat dieses Modell im Mai 1974 auch in einer Stellungnahme für den Innenausschuss des Deutschen Bundestages dargestellt, dessen überarbeitete Fassung er 1975 in der DVR publiziert, siehe Müller (1975b). Für eine ähnliche, wenn auch vereinfachtere Theorie siehe Rachels (1975).

»nicht zur Sache gehören«.“[717] „In dieser Gleichzeitigkeit unterschiedlicher Bilder über einen und *nicht* im generellen Nichtwissen liegt die Struktur der Privatsphäre in Industriegesellschaften begründet; mehr noch: Privatsphäre ist Strukturmerkmal der Sozialbeziehungen selbst.“[718] Für eine rechtliche Regelung gelte daher, dass sie weder auf einem „eindimensionale[n] Kontinuum der Sensitivität von Informationen“ noch auf einer Definition von abgrenzbaren Sphären basieren könne.[719] Stattdessen bedeute das für den Datenschutz eine überlegte, nämlich funktions- und kompetenzorientierte Zuweisung von Informationen für das informationelle Handeln von Institutionen, die Gestaltung von Informationsflüssen und damit „Regelungen der »Informationshaushalte« von Institutionen oder Sektoren der Gesellschaft“.[720] Die empirische Studie, deren Daten Müller neu analyisiert und ausgewertet hat, über die Informationsflüsse zwischen Institutionen wurden von der kanadischen Privacy and Computer Task Force durchgeführt[721] Im Ergebnis stellt Müller fest, dass aufgrund der Datenweitergabe zwischen den Institutionen insbesondere dort „Informationsniveauunterschiede“ verringert würden, wo die meisten Informationen „aus unterschiedlichen Situationen stammen“.[722] Damit werde nicht nur die rollenspezifische Exklusivität der Informationsweitergabe durch Individuen an einzelne Institutionen zerstört, sondern es erhöhe sich auch die Unabhängigkeit von Institutionen von der Kooperationsbereitschaft von Individuen.[723] Anschließend kritisiert Müller die bisherigen empirischen Studien zu den Einstellungen von Individuen zu *privacy*, Privatsphäre und Datenschutz als theoretisch schwach – eine Kritik, die auch heute noch auf die meisten Studien zu diesem Thema zutrifft.[724] Stattdessen verweist er auf die Notwendigkeit von empirischen Untersuchungen zur Messung der „Bereitschaft der Bevölkerung, unterschiedliche Institutionen nur Unterschiedliches wissen zu lassen [...], wie dies das anfangs kurz beschriebene Modell der Privatsphäre in hochdifferenzierten Sozialsystemen erwarten läßt.“[725] Auch Steinmüller betrachtet das Datenschutzproblem als gesellschaftliche Informationskontrolle, als Informationsverteilungskontrolle.[726] Er geht dabei von der Annahme aus, „[d]ie Bedeutung bzw. Leistung von Informationssystemen besteh[e] in

[717] Siehe Müller (1975a, S. 121).
[718] Müller (1975a, S. 121).
[719] Siehe Müller (1975a, S. 122).
[720] Siehe Müller (1975a, S. 123).
[721] Siehe Müller (1975a, S. 125). Die Quellenangabe bei Müller lautet: „Caroll, J. M., and Baudot, J., Kirsh, C., Williams, J. I.: Personal Records: Procedures, Practices and Problems. A Study by the Privacy and Computer Task Force, Kanada: Department of Communications/Department of Justice, o. J.“ Nach Google Books erschien das Buch 1972.
[722] Siehe Müller (1975a, S. 128).
[723] Siehe Müller (1975a, S. 128).
[724] Siehe Müller (1975a, S. 129). Müller verweist dabei etwa auf die dem Younger-Report zugrunde liegende Studie „Survey on public attitudes to privacy“, in der „weder eine theoretische Bestimmung von »Privatsphäre« vorher geleistet wurde noch eine Auswertung der Befunde vorgenommen wurde, die den – ohnehin schwachen – theoretischen Vorüberlegungen auch nur adäquat wäre. Durch solche Vorgehensweisen werden Umfragebefunde tendenziell zum »Kaffeesatz«!“ (S. 129, Fn. 10) Die gleiche Schwäche zeigen bis heute die meisten Studien, die ein „Privacy Paradox“ nachweisen wollen: Es wird weder problematisiert, dass die Forscherinnen begründungslos unterstellen, die von ihnen vertretene *privacy*-Theorie sei deckungsgleich mit der von den Befragten vertretenen, noch dass die von den Forscherinnen vertretene *privacy*-Theorie, die im wesentlichen der von Müller kritisierten dyadischen Gegenüberstellung einer „privaten“ und einer „öffentlichen“ Sphäre bzw. der (daraus abgeleiteten) Trennung zwischen „privaten“ und „öffentlichen“ Informationen folgt.
[725] Müller (1975a, S. 136). Für die dann folgende Behauptung, dass solche Befunde auch verstreut vorliegen würden, gibt Müller allerdings keine Belege an.
[726] Siehe Steinmüller (1975c).

der Erzeugung und Optimierung dynamischer kybernetischer »Modelle« über gesellschaftliche Objekte zu deren Beherrschung.“[727]

> „»Beherrschung« ist hier eine soziologische Kategorie, die alle diejenigen Mechanismen der Planbarmachung, Steuerung und Lenkung der Gesellschaft durch das politisch-administrative System einerseits, durch das ökonomische und das mediäre System andererseits zusammenfaßt, also ein »wertneutraler« Begriff, der noch vor jeder Differenzierung in legitime und illegitime Mechanismen gelten soll. »Systemherr« sei in diesem Zusammenhang jeder, der berechtigt oder unberechtigt über die Leistung des jeweiligen Informationssystems zu verfügen imstande ist.“[728]

Steinmüller unterscheidet zwischen der „quasi-industrielle[n] Bereitstellung von Informationen als Entscheidungshilfe“ und der Kommodifizierung von Informationen und beschreibt die Integrationstendenzen von Informationssystemen vor dem Hintergrund des aufkommenden – später so genannten – Internets aus der „Verbindung der Computer- mit der Nachrichtentechnik“.[729] Weil soziale Interaktion automationshemmend sei, würden „Kooperations- und Partizipationsstrukturen“ zugunsten von Automationsprojekten zurückgedrängt. Nicht nur stehe dies „ausdrücklich in den staatlichen Vorschriften zur Automationsvorbereitung“, sondern folge auch notwendig „aus dem Modellcharakter der Informationssysteme“.[730] Wie Müller verweist Steinmüller dazu auf den tendenziell sinkenden Bedarf nach Rückmeldungen aus der Gesellschaft – „das Modell ersetzt sie“.[731] Damit komme es zu einer Vernichtung von liberalen Freiheitsräumen:

> „Der staatsfreie Raum verschwindet weitgehend: Er ist in Datenform längst als Modell in die staatlichen Informationssysteme aufgenommen – und damit durchschaubar (außer für den Betroffenen), folglich in seiner Funktion beseitigt. – Entsprechendes ist übrigens im wirtschaftlichen Bereich vorgebildet: Erfolgreiches Marketing kennt keine Privatsphäre – wohl aber die Pflege der Illusion darüber; beides ist über ADV zu optimieren.“[732]

In der nachfolgenden Diskussion stellt Harald Weinrich die auch schon von Alan Westin postulierte These auf, dass sich das Datenschutzproblem mit einem „weitergefassten, [. . . .] analogischen Begriff des »Informationseigentums«“ lösen lasse.[733] Steinmüller widerspricht:

> „Hier handelt es sich weniger um Eigentumsverhältnisse als um reale Zuordnungen und normative Berechtigungen zu Verfügung über Informationen. Aus diesem Grund versagt leider der Vorschlag, dem betroffenen Bürger eine Art Eigentumsrecht an seinen Daten zu geben, weil die für die Institution des Eigentums gebildeten Rechtsfiguren für diese wesentlich beweglichere »Sache Information« nicht paßt! Sie ist längst in »Gemeineigentum« übergegangen. . . “[734]

[727] Steinmüller (1975c, S. 142).
[728] Steinmüller (1975c, S. 142).
[729] Siehe Steinmüller (1975c, S. 144).
[730] Im Rahmen der Diskussion deckt Steinmüller dann seinen Begriff von Informationssystem auf: „Ich habe das Wort »System« in der Weise gebraucht, daß es mit dem kybernetischen Organisationsbegriff kompatibel ist.“ Hoffmann et al. (1975, S. 148).
[731] Siehe Steinmüller (1975c, S. 146).
[732] Steinmüller (1975c, S. 146).
[733] Siehe Hoffmann et al. (1975, S. 150).
[734] Hoffmann et al. (1975, S. 151).

Klaus Brunnstein weist in seinem Beitrag darauf hin, dass aus der Kontextabhängigkeit der meisten Informationen folge, dass nur kontextunabhängige Daten gespeichert werden dürften, da es generell unmöglich zu sein scheine, „festzustellen und zu speichern, in welchem Zusammenhang zu einer bestimmten Zeit eine bestimmte Information über eine Person erzeugt worden ist.“[735] Für alle zu speichernden Daten müssten daher „die Interpretationsregeln bei der Benutzung dieser Daten“ definiert und mitgespeichert werden. Wenn es keine „eindeutige Interpretationsregel“ für ein Datum gebe, dürfe das auch nicht gespeichert werden.[736] Auf der Basis der von Carl Adam Petri schon 1962 in seiner Dissertation „Kommunikation mit Automaten“ vertretenen Annahme, dass es sich bei EDV-Systemen um ein „neuartiges, sehr verallgemeinertes Kommunikationsmedium“ handele, mit dessen Hilfe „bisher unübersteigbare Schranken der Kommunikation vollständig niedergerissen werden können“, argumentiert Hartmann J. Genrich, wissenschaftlicher Mitarbeiter der Gesellschaft für Mathematik und Datenverarbeitung, dass „ein Disziplin-loser Einsatz der EDV zu einer erheblichen Störung [...] der auf herkömmlichen Medien und deren Schranken beruhenden Regelkreise führen, welche eine Gesellschaft im Gleichgewicht halten.“[737] Ausgehend von der damals und heute verbreiteten Annahme, beim Datenschutz gehe es um einen Schutz gegen Missbrauch, verweist Genrich zumindest darauf, dass Gegenstand eines solchen Schutzes gegen Missbrauch nur sein könne, dessen Gebrauch festliege: „Für eine geregelte und geschützte Kommunikation kommen genau die Nachrichten in Frage, die einer präzise formulierten und von allen Beteiligten akzeptierten Zweckbestimmung und Handhabung unterliegen.“[738] Beliebiger Gebrauch von Nachrichten sei dasselbe wie „totaler Mißbrauch“.[739] Günter Lemke versucht in seinem Beitrag, anhand von sechzehn Thesen die qualitative Veränderung der Informationsordnung und der daraus folgenden Notwendigkeit einer veränderten Informationspolitik zu belegen.[740] Neben den schon damals überall vorgebrachten Aspekten – Entmaterialisierung, Einmalerfassung und -speicherung, Verfügbarkeit und Benutzbarkeit – identifiziert er Eigenschaften, die bis dahin noch nicht umfassend ausdiskutiert wurden: Aus der Verbesserung der Erschließbarkeit folge, dass das System zur Generierung „ganz neuer Daten aus den bereits vorhandenen Datenbeständen“ in der Lage sei.[741] Auch ließen sich zwischen den Datenbeständen neue Beziehungen herstellen und damit würden „qualitativ neue Daten generiert.“[742] In der Diskussion verweist Horst Oberquelle, der später Informatikprofessor in Hamburg wurde, auf die Problematik der Präjudizierung der Struktur gesellschaftlicher Vorgänge durch die Technikerinnen, etwa „indem die Struktur und Arbeitsweise von Informationssystemen nach technologischen Gesichtspunkten der Informatik bestimmt werden.“ Stattdessen bedürfe es einer „eingehenden öffentlichen und interdisziplinären Diskussion und Entscheidung.“[743]

[735] Siehe Brunnstein (1975, S. 155 f.).
[736] Siehe Brunnstein (1975, S. 156).
[737] Siehe Genrich (1975, S. 158 f.).
[738] Genrich (1975, S. 160). Nachrichten schließen dabei für Genrich „Daten“ und „Informationen“ ein, wie er ebd. erläutert.
[739] Siehe Genrich (1975, S. 160).
[740] Siehe Lemke (1975).
[741] Siehe Lemke (1975, S. 162).
[742] Siehe Lemke (1975, S. 163). Nach Ansicht vieler Beteiligter an der derzeitigen *privacy*- und Datenschutzdebatte sei diese Fähigkeit zur Generierung neuer Informationen aus bestehenden Daten erst mit den neuen Big-Data-Verfahren entstanden. In Wirklichkeit zeigt sich daran nur, dass selbst in der „Wissenschaft“ das Niveau der Debatte unterirdisch geworden ist, weil das Nichtwissen der Unwissenden zum Maßstab der Analyse geworden ist.
[743] Hoffmann et al. (1975, S. 167).

Auch die Deutsche Sektion der Internationalen Juristen-Kommission führte 1974 eine Arbeitstagung zu Fragen „des Schutzes des Freiheitsraumes und der Privatsphäre der Bürger vor jedwedem Mißbrauch der in elektronischen Datenbanken gespeicherten »personenbezogenen« Informationen (sog. Datenschutz)“ wegen der Bedeutung des Themas für „die Bewährung der Rechtsstaatidee – Wissen bedeutet Macht, und Macht bedarf der Kontrolle“ durch,[744] bei der zwei Vorträge gehalten wurden, von Gerhard Löchner, Oberstaatsanwalt beim Bundesgerichtshof, und Steinmüller. Für Löchner besteht das Datenschutzproblem in „der hohen Datenkonzentration an zentralen Stellen“, die „in naher Zukunft eine Verknüpfung dieser Datensysteme miteinander“ erlauben werde. Datenschutz sei also der Schutz vor „Daten-(Macht-)Mißbrauch“, Datenschutz im engeren Sinne sei „ein Instrument zum Schutz des grundgesetzlich geschützten Freiheitsraumes des einzelnen Bürgers vor staatlicher Gewalt und vor Eingriffen anderer Institutionen als Trägern gesellschaftlicher oder wirtschaftlicher Macht“. Datenschutz im weiteren Sinne schütze auch „Gruppen und Verbände“ sowie das Informationsgleichgewicht zwischen den Gewalten, einerseits zwischen Regierung und Parlament, andererseits zwischen Verwaltung und Justiz. Datenschutz müsse daher auch „die Ausgewogenheit der Informationshaushalte der Träger staatlicher oder gesellschaftlicher Macht untereinander sicherstellen.“[745] Für die Frage nach dem Schutzobjekt des Datenschutzes verweist Löchner auf das „Begriffschaos“ der Sphärentheorie, die „Relativität der Privatsphäre“ und die „Stückwerks-Arbeit“ einer kasuistischen Bestimmung der Privatsphäre, um deren Ungeeignetheit zu begründen.[746] Anschließend referiert er die Struktur des Entwurfs des Bundesdatenschutzgesetzes, seine Einzelregelungen und deren Begründung.[747] So weist er etwa darauf hin, dass die Frage, welche Datenschutzmaßnahmen ergriffen werden müssten, „sich dabei nicht nur nach der Art der Daten [richte], sondern [...] auch den Aufbau und die Organisation [der Stelle] und den Datenfluß schlechthin berücksichtigen“ müsse.[748] Abschließend fasst er die offenen Fragen der damaligen Datenschutzdiskussion zusammen: die nach der „konkreten systematischen Form eine[r] wirksamen Kontrolle“ oder die nach der Einbeziehung der „Datenermittlung“ und der nicht in Dateien gespeicherten Daten in das BDSG.[749] In seinem anschließend gehaltenen Referat bezeichnet Steinmüller den Datenschutz „als einseitige Betrachtung eines umfassenderen Problems veränderter Machtstrukturen im Gefolge der Informationsautomation“.[750] Aufbauend auf der Identifizierung der automationsunterstützten Datenverarbeitung (ADV) als „erstmals gelungene Mechanisierung und Maschinisierung geistiger Tätigkeiten“,[751] würden nach Steinmüller erstmals „sogar gesamtgesellschaftliche Steuerung und Regelung mit Hilfe computerunterstützter Informationssysteme und Rechnerverbundnetze in den Bereich des Möglichen“[752] rücken. Zwar könnten „nur Teilaspekte menschlichen Denkens und Lernens durch ADV nachgeahmt (»simuliert«)“[753] werden – nur die formalisierbaren –, allerdings sei dies nur ein temporäres, nicht aber ein grundsätzliches Problem: Langfristig würden all diejenigen „geistigen Funktionen des Menschen“ automatisiert, „an deren Automatisierung ein durchsetzbares Interesse besteht.“[754] Nach einer Darstellung des Auf-

[744] Löchner und Steinmüller (1975, Vorwort, ohne Seite).
[745] Löchner (1975, S. 2 f.).
[746] Löchner (1975, S. 4 f.).
[747] Löchner (1975, S. 5 ff.).
[748] Löchner (1975, S. 15).
[749] Löchner (1975, S. 31).
[750] Steinmüller (1975b, S. 35).
[751] Steinmüller (1975b, S. 38).
[752] Steinmüller (1975b, S. 39).
[753] Steinmüller (1975b, S. 40).
[754] Steinmüller (1975b, S. 41).

baus von Informationssystemen (Hardware, Software, Daten, Organisation, Menschen und die Beziehung zur Umwelt)[755] beschreibt Steinmüller deren Eigenschaften:[756] Geschwindigkeitszunahme, Verringerung der Fehlerquote, weitgehende Aufhebung bisheriger menschlicher Grenzen von Raum und Zeit (Ortsunabhängigkeit, Zeitinvarianz: „Unsterblichkeit“ und Gleichzeitigkeit) sowie die „Gestaltbarkeit und Anpassungsfähigkeit der ADV und ihrer Organisation an die Bedürfnisse des Menschen“.[757] Letztere hält Steinmüller für die „sozial wichtigste Eigenschaft“: „Entgegen gerade von politisch Interessierten häufig aufgestellten Behauptungen kennt darum ADV kaum »Sachzwänge«, die diese oder jene humane oder partizipationsfreundlichere Gestaltung grundsätzlich verböten.“[758] Solche Sachzwänge würden durch die Systemgestaltung erst erzeugt. Besonders deutlich kann dies am Beispiel des von Steinmüller beschriebenen Modells der „integrierten Datenverarbeitung“ gesehen werden:

> „Integrierte DV ist nach der Vorstellung vieler der Idealtypus der ADV; im integrierten IS ist die technische Rationalisierung auf die Spitze getrieben. Sie ist darum, auch wo die völlige Realisierung als utopisch abgewehrt wird, das unausgesprochene Ziel aller technokratisch ausgerichteten ADV: Alle Daten über alle Betroffenen werden nur einmal erfaßt, einmal gespeichert, einmal gelöscht – »Minimierung der Datenmenge« –; alle Daten werden möglichst häufig verarbeitet und weitergegeben sowie möglichst vielen Benutzern zur Auswertung überlassen – »Maximierung der Datenflüsse und DV-Leistung« –; möglichst wenig Programme werden womöglich zentral erstellt, aber möglichst oft weitergegeben und verwendet; alle IS eines bestimmten Raum-Zeit-Gebietes (z.B. Bayern; Hessen; Bundesrepublik) werden möglichst einheitlich organisiert, um eine »modulare« (baukastenförmige) Gesamtorganisation zu einem virtuell einzigen ADV-System zu erreichen, das die Verwertung aller Daten und Programme aller Teilsysteme in einer Hand erlaubt.“[759]

Prinzipielle Leistung von Informationssystemen ist nach Steinmüller die Modellbildung: einmal als „Lernmodell“, einmal als „Entscheidungsmodell“ und als „beide Typen vereinigende[s] Verhaltens-(Simulations-)modell“:

> „Die Gesamtheit der IS [...] bildet tendenziell die Gesamtheit der Gesellschaft, ihrer Teile und ihrer Organisation(en) – einschließlich des Staates selbst – bis herab auf einzelne Personen dynamisch (in ihrem Verhalten) und strukturell (einschließlich ihrer Beziehungen untereinander und zum Staat wie zu anderen Institutionen und zu Sachen) in Informationsform ab und stellt zusätzliche Möglichkeiten zu ihrer gezielten Beeinflussung bereit.“[760]

Steinmüller stellt anschließend die Folgen einer veränderten Machtverteilung, die aus einer Veränderung der Informationsverteilung erwachse,[761] dar:[762] zwischen Legislative und Exekutive zu Lasten des Parlaments mit abnehmender Kontrollierbarkeit der Exekutive; zwischen Exekutive

[755] Steinmüller (1975b, S. 42 ff.).
[756] Steinmüller (1975b, S. 46 ff.).
[757] Steinmüller (1975b, S. 48).
[758] Steinmüller (1975b, S. 48).
[759] Steinmüller (1975b, S. 49).
[760] Steinmüller (1975b, S. 52).
[761] Steinmüller (1975b, S. 54). Information sei, so Steinmüller, Systemkopplung, damit Schaffung von Abhängigkeiten und darauf aufbauend Schaffung zusätzlicher Einwirkungsmöglichkeiten, ebd.
[762] Steinmüller (1975b, S. 56 ff.).

und Judikative; die Nivellierung bisheriger Machtschranken, die aus spezifischen Systemdifferenzierungen erwachsen waren; die Ausweitung der Steuerbarkeit der im IS abgebildeten Entitäten; die Zurückdrängung von Kooperations- und Partizipationsstrukturen; die Ausweitung der Macht der Organisation über ihre Mitglieder; die Reduzierung von Handlungsspielräumen im kollektiven Bereich durch eine Immunisierung gegen Kritik und Reform; eine zunehmende Verflechtung von Staat und Wirtschaft; eine Taylorisierung der Informationsarbeit mit der Unterwerfung des Menschen unter das „strenge[] Ritual der Maschinenlogik“. Als letzte Folge beschreibt Steinmüller „die engere Datenschutzproblematik“ als „die Bedrohung des individuellen Verhaltensspielraums“[763]:

> „Durch die Abbildung bisheriger »Privatsphären« von Individuen und Minderheiten in staatlichen und kommerziellen Informationssystemen bei gleichzeitiger Planbarmachung erhöht sich der Konformitätsdruck auf diese Teile der Gesellschaft.“[764]

Im Ergebnis ist nach Steinmüller die ADV so zu organisieren, „daß die berechtigten Bedürfnisse des Staates und der Wirtschaft derart erfüllt werden, daß der Freiheitsraum der Betroffenen mindestens erhalten bleibt.“[765] Seine Darstellung der konkreten rechtlichen, organisatorischen und technischen Einhegungsmechanismen entspricht im wesentlichen seinen schon andernorts vorgestellten Vorschlägen.[766]

Als Jurist und Mathematiker/Physiker sowie Institutsleiter in der Gesellschaft für Mathematik und Datenverarbeitung (GMD) versucht Herbert Fiedler 1975, die Diskussion um den Datenschutz aus informatischer Sicht zu strukturieren.[767] Er unterscheidet zwischen zwei Wurzeln der Datenschutzdiskussion: einerseits der „»privacy«-Problematik“, andererseits der „»Datenbank«-Problematik“. In ersterer gehe es um „Verletzung[en] einer »Privatsphäre«“ und die „Stellung des Einzelnen in der Gesellschaft“, in letzterer um die „automatisierte Datenverwaltung als technologisches Mittel der Bürokratie in Staat und Wirtschaft“ mit dem Ziel der „Garantie der Transparenz und Beherrschbarkeit der DV-Technologie“. In der Datenschutzdiskussion seien beide Diskussionsstränge „derart zusammengeflossen, daß hier eine Technologie als Antagonist eines Persönlichkeitswerts gesehen wird.“[768] Anschließend unternimmt es Fiedler, die in der Datenschutzdiskussion aufeinandertreffenden „Konflikte mehrere[r] je für sich durchaus legitime[r] Interessen“[769] zu identifizieren: 1. die „Erhaltung der »privacy« im weitesten Sinne“, 2. die „Gewährleistung der Autonomie von Personen, Organisationen und Gruppen durch Einräumung gesellschaftlicher Freiräume“, 3. die „Erhaltung eines »Informationsgleichgewichts« zwischen verschiedenen Instanzen“, 4. die „Gewährleistung der Funktionsfähigkeit und Konkurrenzfähigkeit der Wirtschaft“, 5. die „Gewährleistung der Funktionsfähigkeit und Effizienz in Staat und öffentlicher Verwaltung“ sowie 6. die „Gewährleistung gesellschaftlicher Transparenz und Kontrollfähigkeit“.[770] Er beklagt, dass es trotz des Umfangs der Datenschutzdiskussion an einer

[763] Steinmüller (1975b, S. 66).
[764] Steinmüller (1975b, S. 67).
[765] Steinmüller (1975b, S. 69).
[766] Steinmüller (1975b, S. 67 ff.).
[767] Fiedler (1975). Siehe auch die erweiterte Fassung Fiedler (1976).
[768] Fiedler (1975, S. 71).
[769] Fiedler (1975, S. 73).
[770] Fiedler (1975, S. 74). Dabei ist allerdings völlig unklar, warum er unter 6. schreibt: „Hierher gehört insbesondere die Kriminalitätsprophylaxe, z. B. der Wirtschaftskriminalität.“ Diese Formulierung scheint nahezulegen, dass die gesellschaftliche Transparenz und Kontrollfähigkeit, die Fiedler meint, die Transparenz der und die Kontrollfähigkeit über die Gesellschaft sein soll.

genaueren Analyse und Definition dieser Ziele, ihrer Bewertung und einer Festlegung ihrer Verhältnisse zueinander mangele.[771] Da eine rechtliche Regelung ihren Zweck nur erfülle, wenn sie „operational“ sei, also „praktisch anwendbar, entscheidbar, kontrollierbar“, unternimmt es Fiedler, den Entwurf für das BDSG zumindest auf die Regelungsgegenstände hin zu untersuchen und zu kritisieren, den als „ganz auf das Gegensatzpaar privacy / Effizienz“ zugeschnitten ansieht.[772] Die von Tiedemann und Sasse übernommene Struktur[773] zur Untersuchung der Regelungsgegenstände überzeugt dabei schon deshalb nicht, weil sie nicht einmal alle Aspekte enthält, die Fiedler selbst in seinem Text bis dahin schon angesprochen hatte. So fehlt unter anderem die Frage nach dem Verarbeitungszweck, die er selbst auf S. 69 schon angesprochen hatte, in der Auflistung. Kritik übt Fiedler am Fehlen „operationalisierte[r] Lösung[en] der zugrunde liegenden gesellschaftlichen Interessenkonflikte“ durch die Verwendung von „Formeln wie »Erforderlichkeit«, »überwiegendes Interesse«, »schutzwürdige Belange«“.[774] Sein zentraler Kritikpunkt ist allerdings das Fehlen der Möglichkeit, „Durchführung und Kontrolle von Datenschutzregelungen weitgehend durch DV zu unterstützen“, weil „[n]ach den Einsichten der Lehre von der »automationsgerechten Rechtssetzung« [...] solche Klauseln der Automation nämlich nicht günstig“ seien.[775] Abschließend verlangt Fiedler nach einem „Weg vom Datenschutz zu einem allgemeinen Recht der Information“[776], aufgeteilt in „DV-Organisationsrecht“, „DV-Verfahrensrecht“ und „[m]aterielles Informationsrecht des DV-Bereichs“.[777] Seine Begründung verweist auf die fundamentale Veränderung, die sich mit der modernen Datenverarbeitung ergebe:

> „Nach ihrem gesellschaftlichen Stellenwert bedeutet Datenverarbeitung nicht nur »Rationalisierung«, sondern den Übergang zu einer neuen Stufe der Rationalität. Die DV tritt dem Menschen nicht nur als Werkzeug und spezieller Kommunikationspartner (»Roboter«) gegenüber, sondern reguliert als Organisationsprinzip und Kommunikationsmedium wichtige Lebensvorgänge menschlicher Gemeinschaften. Sie mediatisiert Prozesse der zwischenmenschlichen Verständigung und kann dazu führen, daß die menschliche Lebenswelt nur noch in der Sichtweise einer bestimmten »Verdatung« aufgefaßt wird. Durch ihre allgemeine Verbreitung geht die Informationstechnologie weitgehend bereits in die Konstituierung gesellschaftlicher Verhältnisse ein und ermöglicht es, diese automatisch zu dokumentieren. Computer realisieren den »objektiven Geist« der Gesellschaft nicht nur als statische Struktur, sondern als Medium und als überindividuellen Prozeß.“[778]

Abschließend fordert Fiedler von der Informatik und den Informatikerinnen, seine Schilderungen als Auftrag zu verstehen: „Die DV und die Informationssysteme der Zukunft werden wesentlich von den Forderungen nach Datensicherheit und Datenschutz sowie deren rechtlicher Ausgestaltung bestimmt und im Hinblick darauf konstruiert werden. Die Informatik wird so ein gesellschaftlich höchst wichtiges Betätigungsfeld hinzugewinnen, zugleich aber auch verstärkt mit den

[771] Fiedler (1975, S. 75).
[772] Fiedler (1975, S. 75 ff.).
[773] Siehe Tiedemann und Sasse (1973, S. 75 f.).
[774] Fiedler (1975, S. 77).
[775] Fiedler (1975, S. 77 f.).
[776] Fiedler (1975, S. 79).
[777] Fiedler (1975, S. 81).
[778] Fiedler (1975, S. 80).

Gesellschaftswissenschaften kooperieren müssen."[779] Das Feld der Datensicherheit müsse dabei „die Sicherung der bestimmungsgemäßen Funktion von DV-Systemen einschließen".[780]

Vermittelt über die Deutung von Freiheitsgrundrechten einerseits als individuelle Abwehrrechte und andererseits als „institutionelle Garantie eines bestimmten gesellschaftlichen Sachverhaltes [...], der sich durch einen Zustand grundsätzlicher Freiheit des gesellschaftlichen Raumes vor staatlicher Informationssammlung und -weitergabe auszeichnet", das damit eine „rechtlich abgesicherte soziale Flächenwirkung" habe mit einem „von der Verfassung gewollte[n] Bild der Gesellschaft",[781] und dem Verweis auf die Gleichartigkeit von Einsatz und Wirkung der EDV in Staat und Wirtschaft[782] begründet Eggert Schwan die Notwendigkeit des Datenschutzes „sowohl vor dem Staat als auch vor der Wirtschaft".[783] Aus dem „gewohnheitsrechtlich geltende[n] und zum Rechtsstaatsprinzip gehörende[n] Verfassungsrechtssatz"[784] des Vorbehalts des Gesetzes zieht Schwan die Konsequenz, dass dieser auch auf jede Beschaffung und Weitergabe personenbezogener Informationen durch den Staat anzuwenden sei.[785] Sowohl die massenhafte Erhebung und Speicherung personenbezogener Informationen für Planungszwecke als auch das Erstellen von umfassenden Persönlichkeitsprofilen müsse nach Schwan an einer ordentlichen verfassungsrechtlichen Verhältnismäßigkeitsprüfung – Geeignetheit, Erforderlichkeit, Verhältnismäßigkeit im engeren Sinne – scheitern.[786] Aus dem Auffangcharakter des grundgesetzlichen Anknüpfungspunktes des betrachteten Freiheitsrechts – Art. 2 Abs. 1 GG – folge darüber hinaus, dass es keine vom Schutzbereich ausgeschlossenen personenbezogenen Informationen geben könne.[787]

Mit dem Ziel, die moderne automationsgestützte Informationsverarbeitung umfassend einzuordnen, in ihren Folgen zu analysieren und damit eine fundierte interdisziplinäre „noch kaum begonnene Diskussion [zu] beleben", veröffentlichte Steinmüller 1975 „Bruchstücke einer alternativen Theorie des Datenzeitalters".[788] Ausgehend von den Annahmen, dass Datenschutz „weder ein praktikables Mittel zu publikumswirksamer Absicherung effizienter Datenverarbeitung [sei] noch gar lediglich ein Problem, wie individualistische »Privatsphären« einzelner Mittelschichtangehöriger vor den Folgen der bösen Informationstechnik bewahrt bleiben könnten",[789] behauptet er, dass es „im Kern gesellschaftliche Informationskontrolle [sei] und also ein Problem zieladäquater Systemorganisation".[790] In seinem Versuch, diese Behauptung zu belegen, beschreibt Steinmüller zu Beginn die automationsunterstützte Informationsverarbeitung als „erstmals in größerem Umfang verwirklichte Mechanisierung und Maschinisierung intellektueller Prozesse",[791] die sich daraus entwickelnde Informationsorganisation als „Mensch-»Maschine«-System"[792] mit der spezifischen Leistung der „Erzeugung und Optimierung dynamischer kybernetischer »Modelle« über gesellschaftliche Objekte zu deren Beherrschung"[793] und ihre Folgen im Bereich der Wirtschaft, der öffentlichen Verwaltung und im sozio-kulturellen Bereich sowie mögliche Alternativen, für die

[779] Fiedler (1975, S. 81).
[780] Fiedler (1975, S. 81).
[781] Schwan (1975a, S. 121).
[782] Schwan (1975a, S. 123 f.).
[783] Schwan (1975a, S. 124).
[784] Schwan (1975a, S. 126).
[785] Schwan (1975a, S. 127 ff.).
[786] Schwan (1975a, S. 142 ff.).
[787] Schwan (1975a, S. 146 ff.).
[788] Steinmüller (1975a). Bei den „Bruchstücken" handelt es sich um den Untertitel des Textes.
[789] Steinmüller (1975a, S. 509).
[790] Steinmüller (1975a, S. 510).
[791] Steinmüller (1975a, S. 510).
[792] Steinmüller (1975a, S. 514).
[793] Steinmüller (1975a, S. 521).

er gleichwohl „die Vermutung ihrer relativen Wirkungslosigkeit“[794] behauptet. Im Anschluss an Georg Klaus bezeichnet für Steinmüller Automation „den gesellschaftlichen Prozeß fortschreitender Ersetzung menschlicher Tätigkeiten durch Funktionen künstlicher Systeme“,[795] die im Rahmen von ADV „nicht körperliche, sondern (auch) geistige Arbeit“ „»maschinisiert«“[796] und dabei „nicht nur eine (oder mehrere) *bestimmte* menschliche Tätigkeit(en) nach[ahmt], sondern simuliert *unbestimmt* viele“ – sie sei nicht nur „Informations»maschine«, sondern auch Universal»maschine«“.[797] Die „geistigen Funktionen“ würden damit „vergesellschaftet“: „Sie werden dem individuellen Kontext des einzelnen entnommen und in formalisierten »maschinen«verarbeitbaren Abläufen (in »Programmen«) der Allgemeinheit zur Verfügung gestellt.“[798] Das wichtigste Element der ADV sei dabei nicht die „Maschine“, sondern die „Informationsorganisation“, ein „Mensch-»Maschine«-System“,[799] das seine spezifische Leistung prinzipiell „relativ unabhängig von der Güte des Modells“ erbringe: „Immer wird soziale Realität abgebildet, d. h. verfügbar gemacht, und es ist eine Frage der Funktion und des Einzelfalls, ob »richtige« oder »falsche« Daten (wozu auch die »pragmatisch«, d. h. kontext-falschen Daten zählen) »nützlicher« oder »gefährlicher« für Interessenten und Betroffene sind.“[800] In der Folge entfalten sie „(vor allem) ihre (negativen) Wirkungen (der politischen Einschüchterung und der sozialen Beeinflussung) relativ unabhängig davon, wie »richtig« die Daten, wie »gut« die Verknüpfungen, wie »realistisch« die mathematischen Modelle sind.“[801] Idealtypisch würden in einem solchen System „alle Daten über die »Gesellschaft« [...] nur noch einmal erfaßt und gespeichert“ – „Minimierung der Datenquantität“ –, „aber so häufig wie möglich verwendet, vor allem unter so vielen verschiedenen Gesichtspunkten wie möglich ausgewertet [...], um von einem gegebenen Datenvorrat einen maximalen Nutzen zu ziehen“ – „Maximierung der Datenflüsse und Datenfunktionen“.[802] Bedeutsam sei dabei vor allem die Fähigkeit der ADV „zur Integration aller bisherigen Informations»technologien«“[803] und die „Entwicklung vom Informationssystem zum Informationsverbund und Systemnetzwerk“.[804] Während im Bereich der Wirtschaft Informationen dadurch zur Ware würden,[805] unterliege die ADV im öffentlichen Bereich der „Tendenz [...] zur Aufhebung bisheriger Systemdifferenzierungen“, vor allem solche, „die zugleich grundlegende Organisationsprinzipien der Staatsverfassung darstellen“: zwischen Staat und Wirtschaft, das föderale Prinzip, das Selbstverwaltungsrecht von Gemeinden oder das Gewaltenteilungsprinzip.[806] Im sozio-kulturellen Raume sei die wahrscheinlichere Folge, so Steinmüller, „die Reduzierung von Freiheitsräumen für Kollektive und Individuen“, indem diese verdatet und transparent gemacht gemacht würden:[807] Der Mensch werde „den »Gesetzmäßigkeiten« der Informationssysteme ein-

[794] Steinmüller (1975a, S. 539).
[795] Steinmüller (1975a, S. 510, Fn. 11).
[796] Steinmüller (1975a, S. 511). Steinmüller vorsichtige Verwendung des Begriffs der Maschinisierung, die er durch die Verwendung von Anführungszeichen kenntlich macht, ist hier übernommen.
[797] Steinmüller (1975a, S. 511).
[798] Steinmüller (1975a, S. 513).
[799] Steinmüller (1975a, S. 514).
[800] Steinmüller (1975a, S. 521, Fn. 36).
[801] Steinmüller (1975a, S. 521).
[802] Steinmüller (1975a, S. 524). Mit genau der gleichen Formulierung würde frau in der aktuellen Debatte um Big Data nur minimal für Irritationen sorgen.
[803] Steinmüller (1975a, S. 530, Fn. 60).
[804] Steinmüller (1975a, S. 530).
[805] Steinmüller (1975a, S. 529).
[806] Steinmüller (1975a, S. 532).
[807] Steinmüller (1975a, S. 535).

und untergeordnet“.[808] Steinmüllers Lösung erscheint schon damals utopisch: „Zunächst erforderlich (und z. T. erreichbar) wäre, die gesellschaftliche Informationsverteilung transparent und kontrollierbar zu machen, sodann die immensen Möglichkeiten der Informationstechnologie für die Erweiterung gesellschaftlicher Handlungsspielräume einzusetzen.“[809] Wolf-Dieter Narrs „Anmerkungen zu einigen Thesen von W. Steinmüller“ als „dringender Aufruf zur Diskussion“[810] verhallte allerdings weitgehend unerhört.

Anfang 1976 wurde in der von Podlech und Steinmüller herausgegebenen Reihe „Rechtstheorie und Informationsrecht“ die Dissertation von Christoph Mallmann, „Datenschutz in Verwaltungs-Informationssystemen“, publiziert.[811] In seiner Arbeit versucht Mallmann unter Rückgriff auf Westins „Privacy and Freedom“[812] und Luhmanns „Grundrechte als Institution“[813] eine umfassende Ausarbeitung des Rechts auf informationelle Selbstbestimmung, das er mit „Privatsphäre“ gleichsetzt.[814] Er unterstellt dabei, dass Informationen „ja nie wahllos gesammelt [werden], d. h. die Datenverarbeitung in der öffentlichen Verwaltung erfolgt zweckrational im Sinne *Max Webers*.“[815] In seiner Argumentation stützt er sich maßgeblich auf Luhmanns Adaption der soziologischen Rollentheorie,[816] übersieht dabei allerdings völlig, dass auch Westin sich wesentlich auf rollentheoretische Arbeiten stützte. Mallmanns Formulierung des Rechts auf informationelle Selbstbestimmung als „Recht, über die Abgabe von Individualinformationen selbst bestimmen zu können und zwar hauptsächlich im Hinblick auf den Inhalt der abgegebenen Individualinformation und den Empfänger“[817] entspricht dabei fast wörtlich Westins Definition von *privacy*: „Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.“[818] Ob Mallmann die Definition selbst entwickelt hat, von Luhmann übernimmt oder – über Kamlah und Seidel – von Westin, ist unklar. Wenn Datenschutz tatsächlich nur dem Schutz der informationellen Selbstbestimmung dienen würde, wären Datenschutz und *privacy* damit äquivalent. Zumindest aber sind informationelle Selbstbestimmung und *privacy* Äquivalenzen. Anschließend versucht er, für dieses sozialwissenschaftlich bestimmte Recht in den Grundrechten eine rechtliche Ent-

[808] Steinmüller (1975a, S. 536).
[809] Steinmüller (1975a, S. 539).
[810] Narr (1975).
[811] Mallmann (1976a). Ausweislich des Vorworts und seiner Datierung auf Dezember 1975 wurde die Arbeit zwischen Ende 1971 und 1973 abgeschlossen. Nach Aussagen Lutterbecks war es Christoph Mallmann, der die „informationelle Selbstbestimmung“ erfand und über das Gutachten „Grundfragen des Datenschutzes“ (Steinmüller et al. (1971)) in die Datenschutzdiskussion und letztlich auch in das Datenschutzrecht einführte.
[812] Westin (1967).
[813] Luhmann (1986).
[814] Mallmann (1976a, S. 22).
[815] Mallmann (1976a, S. 32) mit Verweis auf Luhmann (1964b) und Luhmann (1964a). Mallmann ist damit einer der wenigen, die tatsächlich explizieren, wie sehr ihre Konzeption von der Rationalität des Datenverarbeiters abhängig ist.
[816] Mallmann (1976a, S. 53 ff.) mit einer Vielzahl von Verweisen auf Luhmanns „Grundrechte als Institution“, mit der Luhmann die soziologische Rollentheorie, die Dahrendorf Dahrendorf (1965) nach Deutschland importierte, in die Rechtswissenschaft einführte und salonfähig machte. Während Dahrendorf vorwiegend Goffmans individualistischer Interpretation der Rollentheorie folgte, stützte sich Luhmann vor allem auf die strukturalistische Interpretation Parsons und Mertons.
[817] Mallmann (1976a, S. 56). Auf S. 57 folgt dann auch die Formulierung, die die Grundlage für die vom Bundesverfassungsgericht gewählte Formulierung liefert: „Endlich setzt dieses informationelle Selbstbestimmungsrecht für den Bestimmenden die Möglichkeit voraus, von der Abgabe von Individualinformation, ihrem Inhalt und ihrem Empfänger zu wissen.“
[818] Westin (1967, S. 7).

sprechung zu finden,[819] muss im Ergebnis allerdings feststellen, dass die speziellen Grundrechte lediglich Teile davon abdecken und verortet es daher im Auffanggrundrecht des Art. 2 Abs. 1 GG:[820] „Aufgrund funktioneller Aussagen über die Privatsphäre in der Rechtsprechung kann eine grundsätzlich vorhandene Bedeutungsgleichheit mit dem sozialwissenschaftlich gefundenen informationellen Selbstbestimmungsrecht des einzelnen festgestellt werden. Die Fundierung dieses Rechts in Art. 2 Abs. 1 GG – teilweise in Verbindung mit Art. 1 Abs. 1 GG – kann als unstreitig bezeichnet werden.“[821]

In einem Seminar im Januar 1975 wurden politische und gesellschaftliche Möglichkeiten und Gefahren „neuer Formen technisch vermittelter Kommunikation“ – „Kabelfernsehen und Breitbandkommunikation“ – diskutiert, und die Ergebnisse 1976 in einem Sammelband veröffentlicht.[822] Wesentlich war die Feststellung, dass „die Konzentration aller Formen technisch vermittelter Kommunikation auf ein Netz [in den Bereich des Realisierbaren rückt], das gleichermaßen Telefon, Datenfernverarbeitung, »Kabel«-rundfunk und -fernsehen, sowie neuartigen Informationsdiensten und anderen Formen der Kommunikation zur Verfügung stünde.“[823] Gefahren lägen, so Lenk im Vorwort, etwa „in der Verwendung oder Vorenthaltung von Information und von Kommunikationschancen als Mittel der Herrschaft über eine atomisierte Öffentlichkeit“, „die Verwendung von Information zur unmittelbaren Überwachung und Kontrolle menschlichen Verhaltens“ und „die durch die Datenverarbeitung wesentlich gesteigerte Möglichkeit, Informationen über menschliches Verhalten zu aggregieren, mit dem Ziel einer Vorwegnahme von Reaktionen der Beherrschten.“[824]

Unter anderem mit der Möglichkeit, die bei der Nutzung von „Ferneinkauf oder Partizipation an Programmen“ über Individuen anfallenden Informationen „zu dessen systematischer Auswertung für Kontroll- und Planungszwecke“ einzusetzen, beschäftigt sich Otto Mallmann in seinem Beitrag „Soziale Kontrolle durch Breitbandtechnologien“.[825] Er stellt fest, dass Verkaufsstrategien desto effizienter sein können, je transparenter das Verhalten der Verbraucherinnen sei – eine Transparenz, die sich insbesondere im Zuge der Ausweitung des bargeldlosen Zahlungsverkehrs erhöhe.[826] Damit erhöhe sich auch das Manipulationspotential.[827] Gleichermaßen steige die Gefahr, dass die dabei erhobenen und gespeicherten Informationen „für privatwirtschaftliche und staatliche Überwachungssysteme“[828] genutzt würden: von Kreditauskunfteien bis zur Polizei – „[a]uch die sozialen Kontakte der Betroffenen werden transparent.“[829] Informationen, wer welches Fernsehprogramm schaue, welche Dokumente aus Bibliotheken oder Fachinformationszentren anfordere, kurz: „Informationen über individuelle Ansichten und Entwicklungen“ ließen sich für politische Kontrolle nutzen.[830] Abschließend weist Mallmann darauf hin, dass eine Ausdehnung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses auf die Breitbandkommunikation „eine nahezu totale Verhaltenskontrolle“ ermögliche[831] – eine Gefahr,

[819] Mallmann (1976a, S. 58 ff.).
[820] Mallmann (1976a, S. 62 ff.).
[821] Mallmann (1976a, S. 69).
[822] Lenk (1976).
[823] Lenk (1976, S. V).
[824] Lenk (1976, S. VII).
[825] Mallmann (1976b). Die Zitate entstammen S. 126.
[826] Mallmann (1976b, S. 131).
[827] Mallmann (1976b, S. 132).
[828] Mallmann (1976b, S. 133).
[829] Mallmann (1976b, S. 134).
[830] Mallmann (1976b, S. 134).
[831] Mallmann (1976b, S. 136).

die sich inzwischen offensichtlich bewahrheitet hat.[832] Ulrich Dammann analysiert in seinem Beitrag die Folgen des Einsatzes von Planungsinformationssystemen,[833] d. h. „eine computergestützte organisatorische und technische Einrichtung mit dem Zweck, einem oder mehreren Entscheidungsträgern in Verwaltung und Politik planungsrelevante Informationen bereitzustellen und dadurch zur Verbesserung von Planungsentscheidungen beizutragen."[834]

> „Das Planungsinformationssystem ist ziemlich genau das, was der Datenschutzdiskussion lang als Schreckbild der integrierten, zentralisierten Datenverarbeitung vorgeschwebt hat: eine die gesamte Population erfassende, sich permanent verbreiternde, vertiefende und zeitlich verlängernde Sammlung personenbezogener Informationen aus praktisch allen Lebensbereichen, die aus methodischen Gründen (beliebige Auswertung, Erweiterung, Fortschreibung) in disaggregierter Form und mit persönlichen und engmaschigen regionalen Identifizierungsmerkmalen versehen sind, kurzum: eine Super-Dossier-Datenbank, die zwangsläufig auch planungsfremde Interessenten auf den Plan ruft und enorme Mißbrauchsmöglichkeiten eröffnet."[835]

Ein „mit überlegenen Informationsinstrumenten ausgestattete[s] Planungssubjekt" verbessere ihre Position sowohl gegenüber den verplanten Individuen, Gruppen und Organisationen als auch gegenüber konkurrierenden Planungssubjekten, gerade auch dadurch, dass es einem Plan „den Charakter eines in sich geschlossenen Ganzes [verleihe], das partielle Modifizierungen nicht zuläßt" und damit das politische Entscheidungsverfahren weitgehend vorzeichne:[836] „[D]ie Rationalität des technischen Vorgangs [diene] als Ersatz für eine Rationalität der öffentlichen Diskussion".[837] Dammann weist dabei darauf hin, dass sich ein Missbrauch von Planungsinformationssystemen „weder bestimmten Verfahren noch bestimmten Datenbereichen zuordnen" lasse: „Er liegt überhaupt nicht in den Systemleistungen selbst, sondern in einer bestimmten Verwendung derselben im gesellschaftlich-politischen Kontext" und könne nur durch seine vollständige „Transparenz für Parlament und Öffentlichkeit" verhindert werden.[838] Unter Rückgriff auf Vorarbeiten Podlechs[839] fordert Dammann für Planungsinformationssysteme eine Trennung zwischen Betreiber und „Planungsträgern und politischen Entscheidungszentren".[840] Nicht zuletzt fordert er größtes öffentliches Misstrauen „gegenüber Planungsvorschlägen, die keine Alternativen aufzeigen, und gegenüber Modellrechnungen, deren Prämissen nicht offengelegt sind".[841]

Mit ähnlichen Informationssystemen – „integrierten Personalinformationssystemen" – und ihren Folgen für die Mitbestimmung beschäftigt sich Wolfgang Kilian in seinem Beitrag und kommt dabei zu einer vergleichbaren Gefährdungsanalyse.[842] Auch für solche Systeme gelte, dass sie einen Informationsvorsprung veschafften, „denn wer Entscheidungen simulieren oder besser begründen kann, stärkt seine Machtposition gegenüber anderen Entscheidungsinstanzen."[843] Mit

[832] Beckedahl und Meister (2013).
[833] Dammann (1976b).
[834] Dammann (1976b, S. 139).
[835] Dammann (1976b, S. 142).
[836] Dammann (1976b, S. 150).
[837] Dammann (1976b, S. 152).
[838] Dammann (1976b, S. 154).
[839] Siehe etwa Podlech (1973a).
[840] Dammann (1976b, S. 156).
[841] Dammann (1976b, S. 161).
[842] Kilian (1976). Es entbehrt nicht einer gewissen Ironie, dass das Personalinformationssystem für „500 000 englische Beamte und Staatsangestellte" „PRISM" heißt, „Personal Record Information System for Management", siehe S. 166 und Fn. 3.
[843] Kilian (1976, S. 167).

diesen Systemen und insbesondere deren Ankopplung an andere Informationssysteme in Organisationen werde „der Arbeitnehmer und seine Arbeitskraft in größerem Maße disponibel“: „Dem Rationalisierungsgewinn in der betrieblichen Kosten-Nutzen-Analyse steht ein Selbst- und Mitbestimmungsverlust auf der individuellen Ebene gegenüber.“[844]

Fast parallel und in selbstbezeichneter Ergänzung[845] zum Seminar und daraus entstandenen und von Klaus Lenk herausgegebenen Band „Kommunikationsrechte und Kommunikationspolitik“ fand im Februar 1975 in Darmstadt ein von Steinmüller geleiteter Workshop zu „Informationsrecht und Informationspolitik“ statt, dessen Ergebnisse im Jahr darauf unter diesem Titel publiziert wurden.[846] Der dabei entstandene Sammelband soll dabei, wie Steinmüller in der Einleitung formuliert, „Material für weitere Forschungen“ bereitstellen, da das Informationsrecht erst in seinen Anfängen stecke.[847]

Im ersten Beitrag des Bandes versucht Steinmüller, ein Forschungsprogramm zum Informationsrecht zu entwickeln.[848] Er beginnt mit der Beschreibung moderner Informationsverarbeitung als Ergebnis einer langen historischen Entwicklung von der ausschließlich individuellen Informationsverarbeitung über eine beginnende „Transindividualität“ durch „Institutionalisierungen von Sitten, Bräuchen und Recht“, die Erfindung der Schrift und die Entwicklung von Organisationen – „eine gewisse Objektivierung der Information über die Grenzen des Individuums hinaus“ –, die Entwicklung von Universitäten und die Erfindung des Buchdrucks – und damit die Multiplikation der Adressatinnen – bis hin zur „Verwissenschaftlichung aller Lebensbereiche“, der „Standardisierung von Informationserzeugung und -verarbeitung“ und der zunehmenden Rationalisierung. Den (vorläufigen) Endpunkt der Entwicklung stellten die „nicht-mechanischen Informations»technologien«“ dar, die „automationsunterstützte Informationsverarbeitung“, die „sich nunmehr mit der sog. »Breitbandkommunikation«“ verbinde, mit der es möglich werde, „»maschinell« in großen Mengen und unter geringem Zeitaufwand“ zu erzeugen, zu verarbeiten und zu nutzen: „die Informations»maschine« simuliert (mehr oder minder vollkommen) den informationsverarbeitenden Menschen.“[849] Information sei dabei Modell über Systeme oder Prozesse oder beides – „integriertes Modell“ – und Ergebnis eines Informationsprozesses – ein „Prozeß der Erzeugung handlungsrelevanter ideeller Modelle in einem Empfänger über Originale“.[850] Mit der Automatisierung von (Teilen von) Informationsprozessen werde nicht nur der Mensch insoweit ausgeschlossen, gleichzeitig werden „bisherige menschliche »Beschränktheiten« ebenfalls eliminiert“, „wobei selbstverständlich auch Vorteile humaner Schranken mit verloren gehen (können)“.[851] „Durch Formalisierung und Algorithmisierung individueller Problemlösungen[852] und

[844] Kilian (1976, S. 173).
[845] Siehe Steinmüller (1976a, S. IX).
[846] Steinmüller (1976b).
[847] Steinmüller (1976a, S. IX). Steinmüller schreibt über Informationsrecht und Informationspolitik: „ihr Gegenstand ist undeutlich, ihre Methodik und Systematik sind ungeklärt und undiskutiert, ihre Existenz gar noch unbewiesen. Auch war nicht einmal die Vollständigkeit des Überblicks zu erreichen: Es ist ein erster Beginn, kein abgeklärtes Ende.“ Das erklärt auch die durchaus durchwachsene Qualität der Beiträge.
[848] Steinmüller (1976c).
[849] Steinmüller (1976c, S. 2 ff.). Zu den Grenzen der Verwendung von Begriffen aus der Industriegeschichte – „Mechanisierung“, „Maschinisierung“ etc. – für den Bereich der Informationsverarbeitung siehe S. 9, insbesondere Fn. 29.
[850] Steinmüller (1976c, S. 7).
[851] Steinmüller (1976c, S. 7).
[852] Steinmüller bezeichnet damit die „intellektuellen Prozesse“, „geordnete Mengen von Informationen [...], die den Zweck haben, für »Probleme« [– korrekt wäre: Aufgaben –] Lösungswege und Mittel anzugeben (d. h. letzten Endes: Handlungsanweisungen zu geben) und diese Probleme schließlich mit weiteren (materiellen) Informationen zu lösen.“ Siehe Steinmüller (1976c, S. 9, Fn. 29).

durch Systemkommunikation[853] wird Informationsverarbeitung in weit folgenreicherem Maße als z. B. bei Presse und Funk aus ursprünglichen individuell-sozialen Zusammenhängen gelöst, in einem bestimmten Sinn »objektiviert« und für allgemeine Verwendung bereitgestellt (»vergesellschaftet«)", womit einerseits „der Output quantitativ ungeheuer gesteigert" werde, andererseits – qualitativ – „ein bisher unerreichbarer Komplexitätsgrad sozialer Organisation informationstechnisch reduzierbar und damit gesellschaftlich beherrschbar" werde.[854] Steinmüller schreibt der „Informationstechnologie" dabei einen „instrumentalen" Charakter zu.[855] Sie diene „übergeordneten Interessen", verstärke und verändere sie, erzeuge Rückkopplungen. Das sei allerdings trivial, so Steinmüller, und weiter:

> „Problematisch ist vielmehr, in welcher Weise und in welchem Ausmaß bestehende und bekannte Herrschaftsstrukturen durch Informationstechnologien verstärkt oder vermindert werden; mit welchen spezifischen Informationsmitteln sich nunmehr bestimmte Interessen durchsetzen, andere unterdrückt werden; aber auch umgekehrt: wo anzusetzen sei, wenn bestimmte Auswirkungen unerwünscht sind; welche Strategien zu ihrer Verhinderung zu wählen seien, u. s. f."[856]

Erst auf der Basis einer fundierten Analyse könne und müsse dann das Recht seine „Gestaltungs- und Kanalisierungsfunktion" wahrnehmen.[857] Dazu müsse es insbesondere auch über die drei bis dahin dominierenden Themenbereiche – „Datenschutz im engeren Sinne",[858] „Informations»gleich«gewicht zwischen Institutionen" und „das ADV-Organisationsrecht" – hinausgegangen werden.[859] Gegenstand des Informationsrechts seien damit, so Steinmüller, „Informationssysteme und deren Bezug zum gesellschaftlichen Umsystem", wobei Informationssysteme „diejenigen sozialen Systeme [seien], deren Zweck gerade in Informationsprozessen besteht".[860] Die Einbeziehung des Zwecks sei „systemtheoretisch unvermeidlich", da ohne sie „Systeme nicht definierbar (abgrenzbar)" seien. Daraus folge auch, dass „es unter Kontrollgesichtspunkten unerläßlich wird, die Funktion(en) von Informationssystemen hinreichend zu definieren [...], um ihre Transparenz herzustellen".[861] Steinmüllers weitere Ausführungen zur Methodik und Systematik des Informationsrechts liegen außerhalb des Fokus dieser Arbeit.

Auf der Basis von Vorarbeiten Steinmüllers[862] legt Podlech eine „(i. S. der allgemeinen Systemtheorie) modelltheoretische Interpretation des Informationsbegriffs" vor.[863] Danach seien In-

[853] „Kurzbezeichnung für institutionalisierten Informationsaustausch zwischen technisch im Verbund stehenden Informationssystemen", siehe Steinmüller (1976c, S. 4, Fn. 6).
[854] Steinmüller (1976c, S. 9 f.).
[855] Steinmüller (1976c, S. 10 f.).
[856] Steinmüller (1976c, S. 11).
[857] Steinmüller (1976c, S. 12).
[858] Bezeichnenderweise bezeichnet Steinmüller diesen Bereich als „(fälschlich sog.) »Privatsphäre«" – erst also „fälschlich" und dann auch noch in Anführungszeichen – und erklärt, dass die Behauptung, dass „die Datenschutzdiskussion in der BRD ausnahmslos einer privatistischen Verengung zum Opfer gefallen sei – ein häufig deduzierter Vorwurf – [...] leicht durch Lektüre ausgeräumt werden" könne, siehe Steinmüller (1976c, S. 13 und S. 13, Fn. 41). Auf eine solche Lektüre verzichten viele Beteiligte bis heute, wie der unbegründete Vorwurf, das Volkszählungsurteil – und mithin das Datenschutzrecht – sei „für das Analog-Zeitalter geschrieben", siehe Rieger und Kurz (2014), verdeutlicht.
[859] Steinmüller (1976c, S. 13).
[860] Steinmüller (1976c, S. 15).
[861] Steinmüller (1976c, S. 15, Fn. 51). An dieser Erkenntnis mangelt es all jenen „Theoretikerinnen", die Informationen, Informationssysteme und Informationsverarbeitung ohne Rückgriff auf ihren Zweck rechtlich „einhegen" wollen – für beliebige Grade von Einhegung.
[862] Siehe Steinmüller (1972a).
[863] Podlech (1976d).

formationen Modelle von Objekten, also „Abbildungen von etwas für jemand für einen Zweck“[864] und würden damit neben der syntaktischen und der semantischen auch die sigmatische und die pragmatische Dimension einbeziehen, die für das Recht und die Rechtswissenschaft unentbehrlich seien. Informationssysteme ließen sich damit über die Modellbereiche beschreiben, d. h. die „Gegenstandsbereiche“ – Was wird abgebildet? –, die „Adressatenbereiche“ – Für wen wird es abgebildet? –, die „Zweckbereiche“ – Welchen Zwecken dient die Abbildung? – und die „Textbereiche“ – die Daten in verkörperter Form.[865]

Klaus Grimmer analysiert in einem Beitrag den Informationsaustausch innerhalb des öffentlichen und privaten Bereichs sowie zwischen diesen Bereichen darauf, welche Informationen und welche Arten von Informationen unter welchen Bedingungen vor dem Hintergrund welcher Interessen der Beteiligten ausgetauscht werden, und unterzieht sie einer verfassungsrechtlichen Bewertung.[866] Nach einer umfassenden, aber im Ergebnis wenig hilfreichen und quellenlosen Darstellung existierender Informationsverbünde[867] versucht Grimmer, die Voraussetzungen für eine rechtliche Bewertung zu explizieren.[868] Nach einer „Klassifikation von Datenkategorien“,[869] auf die er später keinen Bezug mehr nimmt, beschäftigt er sich mit dem „Begriff und der Rolle der Information“.[870] Grimmer trennt dabei nicht sauber zwischen Information als Prozess und Information als Objekt, wenn er einerseits definiert, Information sei „die Abgabe und/oder Aufnahme von Zeichen sprachlicher und nichtsprachlicher Form in einem Sinngefüge, Bedeutungszusammenhang“ (S. 73), andererseits über die „entscheidungs- und handlungslogische Funktion von Informationen“ schreibt: „Sie ist Bedingung für Handlungen und Entscheidungen.“ (S. 74). Vor dem Hintergrund, dass die „Entfaltungsmöglichkeiten von Individuen, freigesellschaftlichen und staatlichen Organisationen“ von Informationen abhängen, „welche ihnen – oder Dritten über sie – zur Verfügung stehen“,[871] präsentiert Grimmer – wiederum ohne Quellenangaben – die Interessen, die seiner Meinung nach hinter der Einrichtung von Informationsverbünden stehen,[872] nimmt aber jedenfalls für den öffentlichen Bereich begründungslos Kongruenz rechtlich festgeschriebener und realer Interessen an. Darüber hinaus unterstellt er ohne Begründung oder Verweise auf Quellen, dass die „formale Trennung von Staat und Gesellschaft und die Isolierung des Individuums als Person in Staat und Gesellschaft“ „Strukturelemente der Informationsbeziehungen“ seien, dass „[p]rinzipiell [...] faktisch die Freiheit und Privatheit der Information“ gelte und Information „spezifische Form von Eigentum“ sei.[873] Für die rechtliche Würdigung argumentiert Grimmer, dass eine neue juristische Systematik nicht erforderlich sei, „da Informationsbeziehungen der Struktur einer Gesellschaft und ihren Beziehungen entsprechen“, sich also ganz traditionell an rechtlich geschützten Rechtsgütern und Handlungen orientieren könne,

[864] Podlech (1976d, S. 22). Dabei fehlt allerdings die Problematisierung des „von jemand“, siehe Pohle (2014b, S. 89, Fn. 16).
[865] Podlech (1976d, S. 22 ff.).
[866] Grimmer (1976).
[867] Grimmer (1976, S. 67 ff.). Grimmer definiert Informationsverbund als „nicht nur zufälligen Informationsaustausch, sondern die institutionelle Verfestigung von Informationsbeziehungen“, denen auch die Reziprozität fehlen könne, siehe S. 68. Gerade vor dem Hintergrund, dass nur institutionell verfestigte Informationsbeziehungen betrachtet werden sollen, überrascht die Aufnahme von interpersonalen Informationsbeziehungen, siehe S. 70.
[868] Grimmer (1976, S. 73 ff.).
[869] Grimmer (1976, S. 73).
[870] Grimmer (1976, S. 73 ff.).
[871] Grimmer (1976, S. 74).
[872] Grimmer (1976, S. 75 f.).
[873] Grimmer (1976, S. 76).

die erlaubt oder verboten seien.[874] Abschließend untersucht er dann Individual- und Gruppengrundrechte sowie das Staatsorganisationsrecht,[875] um daraus Anforderungen an Informationsverbünde abzuleiten.[876] Obwohl er dabei feststellt, dass weder die kategoriale Trennung zwischen öffentlich und privat noch die Sphärentheorie geeignet ist, fordert er eine „Zuordnung von Informationen zu einem privaten oder öffentlichen Bereich“ per „Rechtsdeklaration“.[877] Staatliches Informationsinteresse solle, so Grimmer, Vorrang vor „[i]ndividuelle[n] Verfügungsrechte[n] über Informationen“ haben, „wo es um die Herstellung gleicher Meinungsbildungs- und Entscheidungsfreiheit geht oder um die Entfaltung organisierter und nicht organisierter Interessen zur Verdichtung von Mitwirkungs- und Legitimationsformen in der Ausübung staatlicher Gewalt“.[878] Informationsansprüche gegen den Staat bedürfen eines verrechtlichen Interesses, wobei es zu keinen einseitigen Begünstigungen kommen dürfe.[879] Im privaten Bereich würden neben Wettbewerbsregelungen das allgemeine Persönlichkeitsrecht und der Zweckbindungsgrundsatz ausreichen.[880]

Paul J. Müller ist, soweit sich das übersehen lässt, der erste, der expliziert, dass die Datenschutzdiskussion, wo sie vor allem von der „Verwaltungswissenschaft juristischer Provenienz“ geführt oder beeinflusst wird, die „Informationsflüsse im Netzwerk informeller Beziehungen“ in oder zwischen „formell verfaßten Institutionen“ ausblendet bzw. durch die Herstellung „kontrollierte[r] und selektive[r] Zugänglichkeit von Informationen“, durch die „informelle Arrangements nicht entscheidungsrelevant“ werden können sollen, ignorieren können will.[881] Im Gegensatz zu Steinmüller und Wolter[882] ist für Müller nicht sicher, ob die „Institutionalisierung des Prinzips »Einmalerfassung + Mehrfachverwendung«“ zu einer Steigerung der Stabilität der betreffenden Institutionen führen und nicht eher zu steigender Störanfälligkeit insoweit, als die „selektive Informationsweitergabe des Bürgers“[883] darauf reagiert, und die „Verzerrungen und Spannungen im Verhältnis Bürger – Verwaltung“ sich auf das Verhältnis zwischen den Verwaltungen ausdehne.[884] Gleichwohl nehme die „Unabhängigkeit der Institutionen von der Kooperationsbereitschaft der Bürger“ zu.[885]

Hans Brinckmann kritisiert die Datenschutzdebatte für ihren individualistischen Ansatz: ihr liege „ein konsequent liberalistisches Grundrechtsverständnis zugrunde, das weder von sozialstaatlichen noch von demokratietheoretischen Ansätzen [...] tangiert oder geprägt“ sei und die „Teilhaberechte auf Information, bedürfnisorientierte Kommunikation und Transparenz öffentlichen wie privaten Handelns“ ignoriere.[886] Die Datenschutzdebatte laufe auf eine Regelung der Verfügung über Informationen über Marktmechanismen hinaus.[887] Brinckmann will „vermuten dürfen“, dass es nur darum gehe, „unternehmerische »Privatheit« [...]gegen [die] Interessen der Mehrheit aufrechtzuerhalten“; es werde „wenig Bezug auf die durchsetzbaren Schutzbedürfnisse

[874] Grimmer (1976, S. 82).
[875] Grimmer (1976, S. 83 ff.), wobei er bei der Analyse der Individualgrundrechte vor allem auf Hubmann (1967), Westin (1967), Schmidt (1974) und Benda (1974) verweist.
[876] Grimmer (1976, S. 88 ff.).
[877] Grimmer (1976, S. 89).
[878] Grimmer (1976, S. 89 f.).
[879] Grimmer (1976, S. 90).
[880] Grimmer (1976, S. 91).
[881] Müller (1976, S. 96 f.).
[882] Vgl. Steinmüller und Wolter (1974).
[883] So Müllers „modifizierte“ rollentheoretische Beschreibung, siehe vor allem Müller (1974).
[884] Müller (1976, S. 97 f.).
[885] Müller (1976, S. 101).
[886] Brinckmann (1976, S. 113).
[887] Brinckmann (1976, S. 114).

der auf abhängige Arbeit und staatliche Sozialleistungen Angewiesenen, noch weniger auf die Informationsbedürfnisse der Mehrheit“ genommen.[888] Darüber hinaus verwirft Brinckmann die in der Datenschutzdiskussion aufgestellte Behauptung von „Organisationsveränderungen und Grundrechtsgefährdungen als Folge der Informationstechnologie“[889] und behauptet stattdessen, dass diese Veränderungen „vielmehr auf exogene Ursachen zurückgeführt werden“ müssen, ohne dafür allerdings eine Begründung zu liefern.[890] Auch in Bezug auf die Folgen der Automatisierung der Informationsverarbeitung für die Organisation der öffentlichen Verwaltung und das Verhältnis zwischen verschiedenen Verwaltungseinheiten gibt Brinckmann den Stand der Debatte sehr einseitig wieder.[891] Sein Hinweis, dass es kaum möglich sein dürfte, „vom einzelnen Individuum und seiner verfassungsrechtlichen Position aus organisationsrechtliche Forderungen zu stellen, die über den Schutz vor totaler Persönlichkeitsreduzierung und über die Aufrechterhaltung unabhängiger Verwaltungskontrollinstanzen hinausgehen“, ist jedoch sehr beachtenswert.[892] Auch seine Beobachtung, dass gerade jene staatlichen „Entscheidungseinheiten“ einen Funktionsverlust hinnehmen müssten, die für die „sich durchsetzenden Planungsanforderungen [...] dysfunktional geworden“, für die Erfüllung anderer Anforderungen – „demokratische Mitwirkung, Ausrichtung auf gesellschaftliche Problemfelder“ – jedoch erforderlich seien.[893]

Ruprecht B. Kamlah versucht in seinem Beitrag, aus den Entscheidungen des Bundesverfassungsgerichts Hinweise „zur Regelung eines materiellen Informationsrechts“ abzuleiten.[894] Zu schützen sei, so Kamlah, das „Menschenbild des Grundgesetzes“ vor dem „Verlust der Menschenwürde durch Totalerfassung der uns betreffenden Informationen“ durch Regelungen „im Sinne der Wertordnung des Grundgesetzes [...], insbesondere im Sinne der einschlägigen Grundrechtsartikel Art. 1 und Art. 2 Abs. 1 GG (Persönlichkeitsrecht) und Art 5 GG (Informationsfreiheit).“[895] Die Besonderheit von Kamlahs Ausführungen liegt darin, dass er zwar einerseits die Relativität der Privatsphäre für alle drei in ihr enthaltenen „Schutzbereiche: die Intimsphäre, den Privat- und den Öffentlichkeitsbereich“[896] aufzeigt und dabei explizit den Verzicht auf „die eine räumliche Schutzvorstellung suggerierenden »Sphären«“[897] fordert, andererseits aber ein Schutzmodell vertritt, das „personenbezogene Informationen je nach ihrer Zugänglichkeit durch die Allgemeinheit entweder [...]schützt oder nicht [...]schützt“[898] Auch für die Abgrenzung des

[888] Brinckmann (1976, S. 114, Fn. 13). Die Kritik hat einen sehr wahren Kern: Die Aufzählung der fälschlich sogenannten „sensitiven“ Informationen – „Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“ (§ 3 Abs. 9 BDSG) – enthält nur genau solche, von deren Nutzung zur Diskriminierung Mitglieder der bürgerlichen Klasse zumindest potentiell betroffen sein können – zugleich aber auch nicht alle, die in der Vergangenheit zur Diskriminierung genutzt wurden, siehe etwa die Kulakenverfolgung in der Sowjetunion (Angaben über Grundeigentum) oder die Intellektuellenverfolgung in Kambodscha (Angaben zur Bildung) –, *und die nicht zugleich die sozial und ökonomisch Schwächeren vor der bürgerlichen Klassen schützen würde.*

[889] Brinckmann baut hier einen Strohmann auf: Der von ihm zitierte Steinmüller beschreibt diese Folgen nicht als Folgen der „Informationstechnologie“ per se, sondern der Art und Weise, wie sie Einführung umgesetzt und die Technik eingesetzt werde.

[890] Brinckmann (1976, S. 117).

[891] Brinckmann (1976, S. 121).

[892] Brinckmann (1976, S. 121). Zum Glück für das Datenschutzrecht und die dort formulierten Anforderungen an die Gestaltung von Organisationen ist schon im Gutachten von 1971 das Staatsorganisationsrecht als „zweite Säule“ direkt fruchtbar gemacht worden, siehe Steinmüller et al. (1971, S. 60).

[893] Brinckmann (1976, S. 131).

[894] Kamlah (1976).

[895] Kamlah (1976, S. 197).

[896] Kamlah (1976, S. 200).

[897] Kamlah (1976, S. 202).

[898] Kamlah (1976, S. 202).

allgemeinen Persönlichkeitsrechts zur Informationsfreiheit sind weder die Ausführungen des Bundesverfassungsgerichts noch die Kamlahs hilfreich: Das Bundesverfassungsgericht betrachtet nur das Informationsrecht der Presse und deren Zweck, Informationen einer allgemeinen Öffentlichkeit zugänglich zu machen; Kamlah stellt diese Beschränktheit zwar fest – „[f]ür das Erheben und Weitergeben von Informationen (außer Veröffentlichung) ist nichts Neues abzuleiten“ –, kann allerdings weder die eigentliche Beschränkung identifizieren – das wäre die Veröffentlichung *durch die Presse* – noch den tatsächlichen Umfang des zu analysierenden Problems – so fehlen etwa *Verarbeiten* und *Nutzen* in Kamlahs Betrachtung.[899]

Adalbert Podlech unternimmt in seinem Beitrag die Formulierung eines Organisationsprinzips zur Gewährleistung der „Erhaltung wichtiger Freiheitsspielräume“: die Trennung von politischer, technischer und fachlicher Verantwortung in automationsunterstützten staatlichen Informationssystemen.[900] Nach Podlech soll dabei das Informationssystem in drei voneinander separate Subsysteme zerlegt werden: das normgebende, das der Benutzerinnen und das der Unternehmerin.[901] Das normgebende Subsystem trage dabei die „politische Verantwortung“ für das Informationssystem und lege Informationsbereich und Informationsbahnen des Systems und die Rechte der Benutzerinnen fest. Die Unternehmerin trage die „technische Verantwortung“ und habe dabei die Aufgabe der Durchsetzung der Informationssicherheit.[902] Und die Benutzerinnen trügen die „fachliche Verantwortung“, d. h. etwa die Korrektheit der Informationen oder die Einhaltung von Fristen sicherzustellen.[903] Mit Hilfe der schon von Steinmüller vorgeschlagenen Programmkontrolle mit seiner Trennung von technischer und fachlicher Verantwortung soll, so behauptet Podlech, auch die Kontrolle der Informationsverarbeitung inklusive der Kontrolle der Erzeugung neuer Informationen aus bereits vorhandenen umsetzbar sein.[904]

Kurz darauf versucht Podlech, „Aufgaben und Problematik des Datenschutzes“[905] umfassend darzustellen, wobei er – wie schon in seinem Entwurf für ein Bundesdatenschutzgesetz[906] – sich wieder nur auf den öffentlichen Bereich konzentriert und den „Datenschutz im Bereich der Wirtschaft und gesellschaftlicher Großverbände wie Parteien, Gewerkschaften und Presse“ einmal mehr „weitgehend“ ausblendet.[907] Er verfolgt mit der Arbeit das Ziel, das gesellschaftliche Problem zu beschreiben, „auf das der Datenschutz Antwort sein soll“.[908] Datenschutz ist dabei nach Podlech Lösung für das „technik-vermittelte[] gesellschaftliche[]“ Problem der „Feststellung und Durchsetzung der Bedingungen, unter denen das Informationsgebaren einer Gesellschaft für die Glieder der Gesellschaft akzeptabel sein kann“, vergleichbar zum „Problem des Verfassungsstaa-

[899] Kamlah (1976, S. 203 f.).
[900] Podlech (1976b).
[901] Podlech (1976b, S. 209 f.).
[902] Podlech spricht von zwei Aufgaben: Verfügbarkeit und Durchsetzung der „Zuordnungsvorschriften“. Seine Beschreibung enthält allerdings Aspekte aller drei Schutzziele der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.
[903] Podlech (1976b, S. 211 f.).
[904] Podlech (1976b, S. 213).
[905] Podlech (1976a).
[906] Podlech (1973a).
[907] Podlech (1976a, S. 23). Nachteilig ist dabei vor allem, dass Podlech es unterlässt, in seiner Darstellung jeweils deutlich zu machen, ob er gerade den nicht-öffentlichen Bereich ein- oder ausschließt.
[908] Podlech (1976a, S. 23). Die in diesem Zusammenhang ausgesprochene Warnung Podlechs hat sich als richtig herausgestellt: Als „juristische Spezialmaterie“, die „nur noch von Spezialisten beherrschbar“ ist, hat die Datenschutz(rechts)diskussion das Datenschutzproblem längst aus den Augen verloren und ist zur Reflexionsfolie bürgerlicher Befindlichkeiten und juristischer Spitzfindigkeiten geworden; es ist nie, wie Podlech schon damals befürchtete, richtig ausformuliert worden, „geschweige denn Reflexionsbesitz der Gesellschaft“ geworden (ebd.).

tes im politischen Bereich und [...] der Kontrolle der Produktionsverhältnisse im wirtschaftlichen Bereich".[909] Vor dem Hintergrund, dass der Staat als „organisierte Großbürokratie" erstens durch die Ausnutzung von Informationsvorsprüngen physische Machtausübung substituieren könne, zweitens dadurch auch die Bedingungen der Konsensbildung manipulieren könne und drittens formelle Entscheidungsstrukturen durch informelle ersetzen könne, bezeichnet Podlech die Aufgabe des Datenschutzes als die Formulierung „informationell beschreibbare[r] Bedingungen legitimer Machtausübung" und der Suche nach Wegen zu ihrer Umsetzung „unter den veränderten ökonomischen und technischen Bedingungen der organisierten Informationsverarbeitung durch Staaten, wirtschaftende Subjekte und gesellschaftliche Großverbände".[910] Daneben formuliert er die Aufgabe noch einmal negativ: Der Datenschutz diene dazu, „einen Gesellschaftszustand zu verhindern, in dem ein Bürger nicht wissen kann, wer wann was zu welchem Zweck über ihn weiß"[911] – eine Formulierung, die hier zum ersten Mal auftaucht und die später in der leicht geänderten Formulierung des Bundesverfassungsgerichts eine gewisse Berühmtheit erlangte. Der Individualdatenschutz diene dabei dem Schutz der individuellen Grundrechte innerhalb des bürgerlichen Verfassungsstaats, sowohl dem Schutz des *bourgeois* wie des *citoyen*, als Individuum wie in seinen „Rollen als Gruppenmitglied".[912] Das durch Art. 1 GG gestützte und durch Art. 2 GG gewährleistete Recht auf (informationelle) Selbstdarstellung als Eigentumsrecht darzustellen, sei dabei ebenso eine Sackgasse wie die Sphärentheorie.[913] Vielmehr will Podlech die weitere Diskussion um die verfassungsrechtlichen Anforderungen an das Datenschutzrecht auf der Basis des Beitrags von Benda führen,[914] wobei in der rechtlichen Umsetzung allerdings neue Wege zu beschreiten seien, weil die bisherigen Regelungen, die sich mit dem Informationsbereich befassten, ausschließlich „wohl definierte soziale Kommunikationssituationen" beträfen wie üble Nachrede, Beleidigung oder Geheimnisverrat, während automationsgestützte Informationssysteme alle Funktionen herkömmlicher Medien in sich vereinen würden und darüber hinaus grundsätzlich pragmatikfrei seien.[915] Zum Gegenstand des Datenschutzrechts müssten daher „die Informationsbahnen der Gesellschaft mit Quelle, Empfänger und Verwendungszweck der Informationen"

[909] Podlech (1976a, S. 24). Nach Podlech sind die drei Probleme miteinander verknüpft, allerdings bedürfe es „einer ausgearbeiteten Gesellschaftstheorie [...], um das Verhältnis der gesellschaftlichen Bedingungen politischer Macht, ökonomischer Verhältnisse und des Informationshaushaltes und die Abhängigkeiten aller drei von der gesellschaftlich vermittelten Technik bestimmen zu können", wobei er keine solche Theorie sieht. Allenfalls für das Problem der gesellschaftlichen Macht gebe es ein konsistentes Modell, so Podlech: „Konzentrierung der diffusen gesellschaftlichen Macht auf den souveränen Staat, um die Machtfrage entscheidbar zu machen [unter Verweis auf Luhmann (1986)]; Entscheidung der Machtfrage durch die Restriktion auf konsensfähige Machtausübung [unter Verweis auf Wilhelm von Ockham]; Bewirkung der Restriktion durch Gewaltenteilung und Kompetenzbindung [unter Verweis auf Montesquieu]", siehe S. 24 f. Hier wird ganz besonders deutlich, wie sehr die Erfahrung mit dem (bürgerlichen) Rechtsstaat die erste Generation der Datenschützerinnen, ihre Analyse des Datenschutzproblems und ihr Lösungskonzept beeinflusst hat.

[910] Podlech (1976a, S. 25).

[911] Podlech (1976a, S. 23).

[912] Podlech (1976a, S. 26 f.).

[913] Podlech (1976a, S. 28 f.).

[914] Podlech (1976a, S. 29) mit Verweis auf Benda (1974).

[915] Podlech (1976a, S. 31). Podlech spricht dabei genau den zentralen Punkt an, an dem sich die fehlende Fundiertheit der derzeitigen Diskussion erweist: Der Inhalt von Informationen ist kein geeigneter Anknüpfungspunkt für das Recht! Podlechs Begründung dafür klingt wie ein aktueller Debattenbeitrag: „Es ist zB [sic!] ohne weiteres möglich, ein politisches Profil von Bürgern herzustellen, das über soziale Indikatoren und ihre statistischen Beziehungen zu politischen Einstellungen allein aus Informationen besteht, die semantisch [...] in politischen Bedeutungsfeldern nicht auftauchen. Man kann statistisch jemanden politisch festnageln, ohne etwas über sein politisches Verhalten im üblichen Sinn zu wissen. Ein Verbot der Sammlung politischer Informationen über Bürger zum Zwecke der Verhinderung politischer Diskriminierung würde also nichts nutzen." Das ist kein Vergleich zu den heute allgemein üblichen Elogen auf den „besonderen Schutz sensitiver Daten"!

sein.[916] Podlech gesteht dabei ein, dass dies nur möglich sei, wenn „inhaltliche Regelungen“ – also materielles Recht – durch „Verfahrens- und Kompetenzregelungen“ – als formelles Recht – ersetzt würden.[917] Die Qualität eines Datenschutzrechts lasse sich – damals wie heute – vor allem anhand der Regelungen im Geheimdienstbereich messen, so Podlech unter Verweis auf Montesquieu – „La liberté politique consiste dans la sûreté“ – und die „technisch ermöglichte Massenhaftigkeit der Überwachung“.[918] Auch mit Blick auf die Erkenntnisse, die das Church Committee zutage förderte, verweist Podlech darauf, dass „[f]reiheitlich-rechtsstaatliche Demokratie [...] durch Kontrolle bedingt [werde] und unkontrolliert gibt es auf Dauer kein korrektes und faires staatliches Verhalten“, wobei schon die Unsicherheit ob deren Korrektheit und Fairness die politische Freiheit der Bürgerinnen beeinträchtige.[919] Podlech formuliert die von ihm identifizierten Anforderungen als „Grundsatz des Erhebungsverbots pragmatikfreier personenbezogener Informationen“, „Grundsatz des Verbots der Zweckentfremdung erhobener personenbezogener Informationen“, „Grundsatz des Löschungsgebots nicht mehr benötigter personenbezogener Informationen“ und „Grundsatz des Verbots sektorübergreifender Informationskontrolle“.[920]

Fast das genaue Gegenstück zu Podlechs Arbeit ist das Werk von Christoph Sasse, „Sinn und Unsinn des Datenschutzes“.[921] Sasse behauptet, die von ihm als die in der damals herrschenden Diskussion identifizierte Gefährdung:

> „Das total durchleuchtete Individuum, dessen Persönlichkeitsprofil von Freund und Feind am jederzeit verfügbaren Informationsbildschirm abgelesen – und verwendet – werden kann, wird zum neuen, den Rechtsstaat bedrohenden Gespenst. Informationsbeherrschung, sei es durch den Staat, sei es durch Private, erscheint als Mittel zur Zerstörung der Freiheit, zur Manipulation des Menschen, zur Potenzierung öffentlicher oder gesellschaftlicher Macht.“[922]

sei übertrieben und schief; stattdessen handele es sich einerseits um ein Problem von Datensicherheit[923] und andererseits um ein Problem übertriebener Befindlichkeit,[924] die beide von einer „Computer-Furcht“, einem „[i]rrationale[n] Mißtrauen gegen neue Techniken“ gespeist würden.[925] Als die übertriebene Befindlichkeit – oder auch das „diffuse[] Gefühl der Bedrohung“[926] – will Sasse mit Habermas und Schelsky „die mangelnde Angemessenheit des eigenen Erfahrungsbereichs, die immer breiteren Schichten die Identifizierung ihrer privaten Interessen mit den gesamtgesellschaftlichen Ordnungen erschwere“ identifiziert haben, die zu einer „Abkehr des einzelnen [...] von einer stets komplexeren Öffentlichkeit“ und einer „Radikalisierung der Privatsphäre“ führen würden.[927] Gleichwohl vermeidet es Sasse trotz aller „Kritik“ an den be-

[916] Podlech (1976a, S. 32).
[917] Podlech (1976a, S. 32).
[918] Podlech (1976a, S. 32 f.).
[919] Podlech (1976a, S. 34). Die Parallele zum informationellen Verhalten privater Organisationen zeigt sich etwa darin, dass das erste echte Datenschutzgesetz – der Fair Credit Reporting Act – die Fairness im Titel trägt und sie zum Gestaltungsziel unter der Bedingung einer strukturellen Machtimbalance zwischen (Kredit-)Organisation und Individuum macht, siehe dazu auch Hoofnagle (2013).
[920] Podlech (1976a, S. 36 f.).
[921] Sasse (1976).
[922] Sasse (1976, S. 7).
[923] Sasse (1976, S. 8). Für die von ihm angesprochene Gefahr der „mißbräuchliche[n] Datenentnahme“ vermeidet Sasse dabei allerdings eine Definition von Missbrauch und präsentiert damit nicht mehr als eine Tautologie.
[924] Sasse (1976, S. 9 ff.).
[925] Sasse (1976, S. 8 f.).
[926] Sasse (1976, S. 12).
[927] Sasse (1976, S. 9 f.).

stehenden Definitionsversuchen konsequent, eine eigene fundierte allgemeingültige Analyse des Datenschutzproblems vorzulegen: Weder seine tautologisch definierte Aufgabenstellung des Datenschutzes als Missbrauchsverhinderung noch seine Ausführungen zur „Privatsphäre“ können als fundiert bezeichnet werden. Zumindest für den Bereich des Datenschutzes gegenüber der öffentlichen Verwaltung übernimmt er die an verschiedenen Stellen aufgestellte Behauptung, in Datenverbünden würden auch Sammlungen von personenbezogenen Informationen unterhalb der Schwelle von Persönlichkeitsprofilen eine „Nacktheit vor der Verwaltung“ bewirken, die „selbst ohne Mißbrauch, schlicht infolge ihres Vorhandenseins, auf Seiten der Individuen zu einem Spontaneitätsverlust führen würde[n]“, „die Unbefangenheit von Lebensäußerungen“ beeinträchtigen und „mausgraues Anpassungsverhalten“ erzeugen würde, die „mit dem Prinzip demokratischer Ordnung (Art. 20 GG) [...] als unvereinbar gelten“ müsse.[928] Vor diesem Hintergrund vergleicht er dann die Regelungen des Schwedischen Datenschutzgesetzes von 1973 und des Privacy Act of 1974 mit den Entwürfen für das österreichische und das deutsche Datenschutzgesetz in den Bereichen 1. Erheben und Speichern, 2. Weitergabe und 3. Kontrollmechanismen und kommt dabei zum Schluss, dass der deutsche Entwurf in allen Bereichen die schwächsten Regelungen und die größten Regelungslücken enthalte.[929]

Für den privaten Bereich geht Sasse signifikant anders vor. Er beginnt mit einer Darstellung der informationsbezogenen Interessenkonstellation im Kredit-, Versicherungs- und Arbeitsbereich und behauptet, Aufgabe des Datenschutzes sei der Interessenausgleich.[930] Ein Datenschutzrecht für den privaten Bereich dürfe und müsse es aber nur geben, „wenn von der Datenverarbeitung durch Private ähnliche Gefahren ausgehen wie von derjenigen durch die öffentliche Hand.“[931] Und genau dem widerspricht Sasse und behauptet, dass es in der Bundesrepublik keine zu den Fällen in den USA, die in Presse und Literatur angeführt werden, vergleichbaren Fälle geben würde.[932] Die von ihm als Begründung für das Fehlen solcher Fälle in der Bundesrepublik gelieferte Erklärung beschränkt sich allerdings ausschließlich auf den Kreditbereich,[933] während sowohl der Arbeits- als auch der Versicherungsbereich mit ihrer langen Tradition von Schwarzen Listen schlicht nicht betrachtet werden.[934] Sasses Schlussfolgerung, „[d]ie Privatsphäre [sic!] des Staatsbürgers [sic!] ist also diesseits des Atlantik [sic!] weniger gefährdet als in den USA“, führt ihn zu der Forderung, dass der Gesetzgeber, bevor er Datenschutzregelungen für den nicht-öffentlichen Bereich erlasse, „mit Rücksicht auf diese ganz anderen Rahmenbedingungen einige Vorfragen entscheiden“.[935] Diese „Vorfragen“ – oder auch: „Vorentscheidungen“ – expliziert Sasse dann nicht, scheint damit aber Fragen des Geltungsbereichs des Datenschutzgesetzes und Grundentscheidungen bzgl. der rechtlichen Operationalisierung zu meinen: Erstens bestreitet Sasse die – vor allem mit ihrer Relativität begründete – Untauglichkeit des Konzepts der Privatsphäre, da Rechtsprechung und Literatur jedenfalls in der Lage seien, diesen unbestimmten Rechtsbegriff zu objektivieren.[936] Die Verwendung des personenbezogenen Datums als Regelungsobjekt sei entschieden zu umfassend, wo doch – nur – „[e]ine »unantastbare Sphäre

[928] Sasse (1976, S. 12 ff.).
[929] Sasse (1976, S. 20 ff.).
[930] Sasse (1976, S. 27 ff.).
[931] Sasse (1976, S. 29).
[932] Sasse (1976, S. 29 ff.).
[933] Sasse (1976, S. 32 ff.).
[934] Selbst wenn unterstellt wird – was durchaus zweifelhaft erscheint –, dass Sasses Vergleich historisch erstens korrekt und seine Schlussfolgerung zweitens valide ist, haben sich alle aufgeführten Aspekte inzwischen fundamental gewandelt.
[935] Sasse (1976, S. 44).
[936] Sasse (1976, S. 45 f.).

privater Lebensgestaltung« [...] gewährleistet werden“ solle.[937] Und zweitens behauptet Sasse, es gehe im Bereich der gewerblichen Wirtschaft nicht „um die Sphäre individueller Lebensgestaltung oder dergleichen, sondern um die Minimierung von Verlusten, die der Volkswirtschaft insgesamt unerhörten Schaden zufügen.“[938] Und er ergänzt begründungslos: „Für den hierzu erforderlichen Informationsfluß passen die Instrumente des Datenschutzes nicht.“[939] Seine eigene – offenkundig absichtlich beschränkte – Wahrnehmung des Datenschutzproblems als tumbe „»Radikalisierung« der Privatsphäre“ zugrunde legend behauptet Sasse dann, es fehle „an einer sozialpsychologischen oder gesellschaftspolitischen Rechtfertigung“ für eine Anwendung des Datenschutzrechts auf das Verhältnis zwischen „Gewerbetreibenden“.[940] Für den nicht-öffentlichen Bereich fordert Sasse daher eine Zweiteilung: einen individuellen[941] und einen gewerblichen, wobei erster einen – wenn auch untauglichen[942] – verstärkten Schutz genießen solle, während letzter keiner neueren Regelungen bedürfe.[943]

Vor dem Hintergrund von Sasses Argumentation, durch eine signifikant eingeengte und gleichzeitig verzerrte Definition des Datenschutzproblems als Problem einer Privatsphäre monadischer Angehöriger der bürgerlichen Klasse das Datenschutzrecht als Mittel zur gesellschaftlichen Informationsmachtkontrolle[944] leerlaufen zu lassen, erscheinen seine „Schlussfolgerungen“ – „[d]ie Überwachung des öffentlichen Bereichs ist zu matt, der Schutz der Sphäre des Privatmanns zu schwach und konturenlos, und der Datenschutz in der Wirtschaft schießt weit übers Ziel hinaus“[945] – weniger als Schlussfolgerungen einer wissenschaftlichen Analyse als vielmehr als notwendiges Ergebnis von ideologisch beschränkten und sich selbst beschränkenden Annahmen über die bürgerliche Gesellschaft und das bürgerliche Individuum.

In der zweiten Hälfte der siebziger verstärken auch die interdisziplinären Diskussionsforen ihre Hinwendung zu Einzelproblemen der Umsetzung von Datenschutz und Datenschutzrecht auf der einen und Datensicherheit auf der anderen Seite in Technik und Informationsverarbeitungspraxis.[946] Hans-Peter Gassmann ist wohl der erste, der eine explizite Verbindung zwischen dem Problem des Datenschutzes und dem des Umweltschutzes zieht: Moderne Informationsverarbeitung und insbesondere internationale Datenflüsse würden die „Gefahr der Verschmutzung unserer Informationsumwelt“, einer „Informationsumweltverschmutzung“, bergen.[947]Dammann vergleicht die Institutionalisierungsansätze von Datenschutzkontrolle in den USA, Schweden, aber auch Hessen miteinander und stellt fest, dass Datenschutzbeauftragte als „»persuasive au-

[937] Sasse (1976, S. 47) unter Verweis auf die »Amtl. Begr. zum BDSchG-E, Drucks. BR 391/73, Allg. Teil. Nr. 1.1.2.1., 2.3., 3.5. 3.7.«. Oder auch: „[d]as vernünftige Ziel eines verstärkten Schutzes des Einzelnen gegen zudringliches und oft ungenaues Ausforschen seines Privatbereichs“, siehe S. 49.

[938] Sasse (1976, S. 48).

[939] Sasse (1976, S. 48). Es handelt sich offenkundig nicht um ein Problem der Angemessenheit der Instrumente, sondern darum, ob die Informationsflusskontrolle politisch oder ideologisch gewünscht ist.

[940] Sasse (1976, S. 48).

[941] „Wo der Privatmann als Verbraucher, Versicherungsnehmer oder Arbeitssuchender betroffen ist, gilt es wegen der Nähe zur Person, [...]“, siehe Sasse (1976, S. 50).

[942] Nach Sasse soll der Schutz auf der Verwendung korrekter und der nur ausnahmsweisen Verwendung „sensitiver“ – „nämlich Intimdaten, solche über den Gesundheitszustand und über politische oder weltanschauliche Ansichten“ – Informationen basieren, siehe Sasse (1976, S. 50). Sasse hat also, wie viele andere auch, das Problem der pragmatischen Dimension von Information nicht verstanden.

[943] Sasse (1976, S. 50 f.).

[944] Siehe dazu etwa von Lewinski (2009).

[945] Sasse (1976, S. 52).

[946] Dierstein et al. (1976).

[947] Gassmann (1976, S. 14).

thority«, als Autorität durch Überzeugung“ bezeichnet werden könnten.[948] Gleichwohl begnüge sich die Datenschutzkontrollinstanz nicht mit der Aufdeckung und Ahndung von Verstößen, ihr Schwerpunkt liege vielmehr in der präventiven Analyse und Beseitigung von Gefahren.[949] Die von Dammann wiedergegebene Beobachtung, dass „die Aussichten, mit vertretbarem Aufwand zu effektiven Datenschutzmaßnahmen zu kommen, dann besonders groß sind, wenn sie bereits im Zusammenhang mit der Planung eines Informationsvorhabens konzipiert werden“,[950] überrascht daher nicht. Josef Gärtner schlägt für den privaten Bereich die Einführung einer Gefährdungshaftung, eine Beweislastumkehr zugunsten der Betroffenen sowie einen Ersatz auch für immaterielle Schäden vor, wobei die Beweislastumkehr auch bei der Durchsetzung von Unterlassungsansprüchen gelten solle.[951] Nicht nur der Entwurf des deutschen Datenschutzgesetzes,[952] sondern auch der Entwurf des österreichischen Datenschutzgesetzes setze stark auf unbestimmte Rechtsbegriffe, so Herbert Wegschneider. Dabei seien die Begriffsbestimmungen „unklar, widersprüchlich oder gar nicht sinnvoll interpretierbar“.[953] Fred Jaster beschreibt drei Gruppen von Maßnahmen, mit Risikofällen umzugehen: 1. Verhinderung, 2. Erkennung und 3. Beseitigung der Folgen, wobei seine Darstellung nur so gelesen werden kann, dass diese Einteilung offensichtlich schon damals als klassisch gilt.[954] Seine Begründung, warum er ausschließlich Innentäterinnen betrachtet – weil alle „bekannt gewordenen Fälle [...] ausschließlich von diesem Personenkreis verübt“ wurden[955] –, kann zwar heute für den IT-Sicherheitsbereich als überholt angesehen werden, jedoch aber gerade nicht für den Bereich des Datenschutzes, der sich primär mit dem Innenverhältnis zwischen Datenverarbeiter und Betroffener beschäftigt. Bruno Losbichler untersucht, welche Konzepte Programmiersprachen aufweisen sollten, damit sich „für alle im Verlauf der Programmausführung behandelten Objekte problem- und datenspezifische Schutzmaßnahmen formulieren lassen, die während der Programmausführung eingehalten werden“.[956] Er will das mit Hilfe von Spracherweiterungen umsetzen, die ähnlich funktionieren sollen wie die Zuweisungen von Typ- und Strukturinformationen oder Anfangswerten.[957] Jan Schlörer analysiert das Problem der Anonymität in statistischen Datenbanken. Er trennt dabei zwischen Anonymisierung – identifizierende Informationen werden nicht gespeichert – und „funktioneller“ Anonymisierung, bei der die identifizierenden Informationen zwar gespeichert sind, jedoch nicht herausgegeben werden,[958] und identifiziert zwei Gruppen von notwendigen Sicherungen für statistische Datenbanken: Datentransformation und Dialogsicherungen.[959] Datentransformationen seien danach „Veränderungen der Daten selbst, nach deren Durchführung statistische Auswertungen, wenn auch mit verringerter Effizienz, noch möglich, Identifikation von Einzelpersonen

[948] Dammann (1976a, S. 65).
[949] Dammann (1976a, S. 67).
[950] Dammann (1976a, S. 61).
[951] Gärtner (1976, S. 71 ff.).
[952] Sasse (1976, S. 49 f.).
[953] Wegscheider (1976, S. 84).
[954] Jaster (1976, S. 128).
[955] Jaster (1976, S. 128).
[956] Losbichler (1976, S. 139).
[957] Losbichler (1976, S. 143 ff.). Für die aktuelle Diskussion ist mir kein Beitrag bekannt, der auf einer so tiefen Ebene versucht, Datenschutz und Datensicherheit technisch zu lösen. Hinsichtlich seiner Erläuterung und Begründung entspricht der Vorschlag wohl am ehesten den aktuellen *Privacy*-Middleware-Vorschlägen.
[958] Schlörer (1976, S. 155).
[959] Schlörer (1976, S. 156 f.).

aber mehr oder weniger erschwert ist“[960] Auf der anderen Seite seien Dialogsicherungen etwa „Outputmodifikationen“ oder das Nichtbeantworten bestimmter Anfragen zum Ausschluss von „Vertraulichkeitsbrüchen“.[961] Die von Schlörer beschriebenen Ansätze werden heute im Datenbankbereich etwa unter dem Namen „differential privacy“ diskutiert.[962] Lotte Tuner beschäftigt sich mit der Bedeutung des Formularwesens für den Datenschutz.[963] Zentrale Eigenschaft des Formularwesens sei die ihr innewohnende Schematisierung, die „gewaltsame Subsumtion eines normfernen Sachverhalts unter ein Muster, das gerade zur Hand ist“[964], und stelle zugleich eine generelle Fehlerquelle dar, sei gleichwohl aber Grundbedingung für „stärkste Arbeitsteilung und routinemäßige Bearbeitung“.[965] Die Verwendung von Formularen führe – bei Papierformularen über den Vordruck, bei digitalen Formularen über die Beschreibung neben dem Formularfeld bzw. eine kontextuelle Hilfefunktion – zur Suggestion bestimmter Antworten oder Formulierungen von Antworten.[966] Das habe vor allem dann negative Konsequenzen, wenn auch der organisationsinterne Informationsfluss über solche Formulare organisiert ist:

> „Wenn z. B. eine behördliche Auskunft nur unter bestimmten Voraussetzungen erteilt werden darf und ein Vordruck eine Reihe solcher Voraussetzungen in der richtigen Formulierung zur Auswahl stellt, wird der Beamte u. U. unter Vermeidung der wahren Begründung die Auskunft nach dem erfolgversprechendsten System anfordern und erhalten. [...] Müßte der Beamte die Begründung selbst formulieren, könnte u. U. die Auskunft aus datenschutzrechtlichen Gründen verweigert werden.“[967]

Jedoch brächten Formulare aus Datenschutzsicht auch Vorteile mit: Nichts könnte – weder unbeabsichtigt noch absichtlich – vergessen werden, weder Fragen, Mitteilungen, Aufgaben, noch Vorgänge, und die Betroffenen könnten durch Formulare umfänglich und erschöpfend über Möglichkeiten und Risiken der Informationsverarbeitung informiert werden.[968] Ein modernes Formularwesen müsse dabei folgende Anforderungen erfüllen: 1. Vereinheitlichung des Formularwesens, 2. Normierung der verwendeten Begriffe, 3. gesetzlich festgelegter Katalog datenschutzrechtlich zulässiger Fragen (Zweckentfremdungs- und Übermaßverbot) oder Formblattregister mit Genehmigungspflicht für Formulare, 4. Angabe von Zweck und rechtlicher Grundlage, 5. Verständlichkeit der Formulierung, 6. Angaben zur Weitergabe von Daten, 7. Angaben von Art und Ausmaß der Sanktionen bei Nicht- oder Falschausfüllung, 8. grundsätzliche Ausfertigung von Doppeln für die Betroffenen. Als zentrales Gestaltungsziel für Formulare benennt Tuner, dass diese in Bezug auf den Datenschutz als auch im Hinblick auf die Verständlichkeit so zu

[960] Schlörer (1976, S. 157). Seine Lösungsvorschläge umfassen etwa Stichproben anstelle von Populationen, Variableneliminierung, Vergröberung der Klasseneinteilung der Variablen, Datenaggregation oder Einfügen von Zufallsfehlern.

[961] Schlörer (1976, S. 157).

[962] Dabei handelt es sich bei den im Datenbankenbereich diskutierten Anonymitätskonzepten um ausschließlich funktionelle Anonymisierungen im Sinne Schlörers.

[963] Tuner (1976). Auch heute noch sind trotz aller Fortschritte in der Analyse von Volltexten, Bildern oder Tönen sehr viele Systeme Formularverarbeitungssysteme im Tunerschen Verständnis. Tuners Ausführungen sind daher immer noch verständnisfördernd. Formulare sind daher im Folgenden alle strukturgebenden – und mglw. strukturerzwingenden – Dateneingabe- und -speichersysteme, die die strukturierenden Meta-Daten im Verlauf der Informationsverarbeitung mitführen.

[964] Tuner (1976, S. 256 f.).

[965] Tuner (1976, S. 254).

[966] Tuner (1976, S. 260).

[967] Tuner (1976, S. 260 f.).

[968] Tuner (1976, S. 261 ff.).

entwerfen seien, dass Informationsflüsse minimiert werden.[969] Hanns-Wilhelm Heibey, Bernd Lutterbeck, Sabine Rohlfs und Michael Töpel analysieren die Grundlagen und den Charakter moderner Informationsverarbeitung in Organisation und stellen fest, dass der EDV-Einsatz sich „stets im Rahmen der Informationsverarbeitung in organisatorischen Aufgabenlösungsprozessen“ vollziehe.[970] Dabei seien Organisation „Systeme zur Lösung von Aufgaben“, umgesetzt durch arbeitsteilige Ausführung von Einzelaufgaben, wobei im Rahmen dieser Aufgabenlösungsprozesse Informationsverarbeitung stattfinde.[971] Gleichwohl bestehe trotz jahrelanger Diskussion „Unklarheit über zentrale Begriffe wie Information, Daten, Informationsverarbeitung und den Gegenstand, der geschützt werden soll“, d. h. das Schutzgut,[972] wobei sie für die zentralen Begriffe auf Bekanntes zurückgreifen – syntaktische, semantische und pragmatische Ebene von Informationen, während Daten nur die syntaktische Ebene beschreiben[973] – und zum Problem des Schutzgutes keine Ausführungen machen. Computereinsatz begünstige „Zentralisation [sic!] von Entscheidungskompetenzen an der Spitze der Organisationshierarchie“, und mit der „Standardisierung und Routinisierung von Aufgabenlösungsprozessen vermindert sich der Spielraum und damit auch die organisatorische Bedeutung der Dispositionsaufgaben der mittleren Entscheidungsinstanzen“.[974] Es gebe eine „Tendenz zur Abnahme der Flexibilität bei der Anpassung an Umweltveränderungen“, einen Verlust an Transparenz und einen „»Glaube« an die Richtigkeit computerisierter Entscheidungen“.[975] Im Ergebnis sehen die Autorinnen die Datenschutzdiskussion als mehr oder weniger gescheitert an.[976] Dabei bleibt allerdings unklar, ob sie damit die Datenschutz*rechts*diskussion meinen, die bekanntlich kurz darauf in das BDSG mündete, oder die Datenschutzdiskussion im engeren Sinne. Podlech erweitert seine Darstellung der „Aufgaben und Problematik des Datenschutzes“[977] um einige historische und gesellschaftstheoretische Aspekte.[978] Während die entscheidende Leistung des Frühbürgertums gewesen sei, „gegen die feudale Rechtsordnung die Verwandlung menschlicher Arbeitskraft in die Warenform durchzusetzen“, sei die „Verwandlung der Information in die Warenform“ das Kennzeichen der postindustriellen Gesellschaft. Mit der „Verwandlung der Personen repräsentierenden Informationen in die Warenform werden Menschen über ihre Arbeit hinaus aller Möglichkeiten entfremdet, sich selbst, ihre Vergangenheit und ihre Zukunft frei in gesellschaftlicher Kommunikation darzustellen.“[979] Als notwendige Bedingung der Akzeptabilität des Informationsgebarens einer Gesellschaft für die Glieder der Gesellschaft bezeichnet Podlech „die Gewährleistung der Sicherheit und der Selbstdarstellungschancen.“[980] Neben die schon vorher formulierten Grundsätze – „Erhebungsverbot pragmatikfreier personenbezogener Informationen“, „Verbot der Zweckentfremdung erhobener personenbezogener Informationen“, „Löschungsgebot nicht mehr benötigter personenbezogener Informationen“ und „Verbot sektorübergreifender Informationskontrolle“[981]

[969] Tuner (1976, S. 264).
[970] Heibey et al. (1976, S. 298).
[971] Heibey et al. (1976, S. 300).
[972] Heibey et al. (1976, S. 299).
[973] Heibey et al. (1976, S. 300).
[974] Heibey et al. (1976, S. 302 f.).
[975] Heibey et al. (1976, S. 303).
[976] Heibey et al. (1976, S. 308).
[977] Podlech (1976a).
[978] Podlech (1976c).
[979] Podlech (1976c, S. 315 f.).
[980] Podlech (1976c, S. 317). Mit „Sicherheit“ meint er dabei „sûreté“, die Sicherheit vor dem Staat, und verweist dazu auf Art. 3 Abs. 3, Art. 4, 5, 8, 9, 12, 33 Abs. 2 und 3 GG. Für die Selbstdarstellungschancen verweist er auf Art. 1, 2 Abs. 1, Art. 4, 5, 6, 10 und 13 GG.
[981] Podlech (1976a, S. 36 f.).

– stellt er drei neue: den „Grundsatz der Fremdkontrolle geheimdienstlicher Informationsübermittlung“,[982] den „Grundsatz der Primärerhebung personenbezogener Informationen“[983] und den „Grundsatz des privaten Verwertungsverbotes personenbezogener Informationen“ mit dem Ziel der „Verhinderung der Verwandlung von Personen im sozialen Kontakt darstellenden Informationen in die Warenform und die Verhinderung der durch diese Verwandlung eintretenden Entfremdung.“[984] Abschließend zeigt er an Beispielen aus der jüngeren Geschichte die Notwendigkeit des Datenschutzes:

> „Unberührt von dem skizzierten Lösungsmodell bleibt der Alptraum des Datenschutzes angesichts der inhumanen politischen Geschichte unseres Jahrhunderts. Man stelle sich vor, in den europäischen Staaten hätten seit Beginn unseres Jahrhunderts integrierte vollständige Informationssysteme der öffentlichen Verwaltung bestanden. Was wäre 1909 (Türkei), 1910 (Portugal), 1917 (Rußland), 1918 (Deutschland, Österreich-Ungarn), 1922 (Italien), 1925 (Portugal), 1931 (Zypern), 1933 (Deutschland), 1936 (Griechenland, Spanien), 1939 ff. (Europa, Nazifizierung), 1943/45 (Europa, Entnazifizierung), 1947 (Ostblockstaaten), 1950 (Türkei), 1956 (Ungarn), 1960 (Türkei), 1967 (Griechenland), 1968 (Tschechoslowakei), 1974 (Portugal, Griechenland), zusätzlich geschehen, wenn Bürger hinsichtlich ihres gesellschaftlichen Verhaltens so erfaßt gewesen wären, wie es solche Informationssysterne ermöglichen. Ich hege nicht die Zuversicht, daß dieser retrospektive Alptraum nicht eines Tages für Bürger ein prospektiver Alptraum werden könnte.“[985]

In einer auf seiner Habilitationsschrift basierenden Arbeit „Der verfassungsrechtliche Schutz der Privatheit“ versucht Giselher Rüpke, das vom Persönlichkeitsrecht geschützte Rechtsgut, das er „Privatheit“ nennt und mit „privacy“ gleichsetzt,[986] auf der Basis von Anleihen aus der Sozialpsychologie, der Symbol- und der Sprachtheorie zu bestimmen, vor allem auf der Basis des symbolischen Interaktionismus. Er unterscheidet zwischen Information und Kommunikation, wobei er Informationen als „bezogen auf Inhalte oder feststehende Bedeutungen“ und Kommunikation als „die in der je einzelnen sozialen Situation spezifische symbolische Vermittlung und der damit verbundene pragmatische Sinn“ betrachtet,[987] um dann darauf aufbauend zwar nicht Privatheit zu bestimmen, aber zumindest dessen Funktion:

> „Bei enger Bindung ist die Kommunikation außerhalb des »Kontextes«, der spezifischen sozialen Beziehung, nicht (voll) verständlich; Privatheit soll sehr wahrscheinlich gegen »Mißverständnisse« im weitesten Sinn, gegen Fehlinterpretation, Entstellung und gegen Umkehrung des pragmatischen Sinns, Entfremdung des symbolisch-immanent festgemachten »Zwecks« der Kommunikation schützen.“[988]

Als Schutzgüter von Privatheit nennt Rüpke dann die „Spontaneität der Kommunikation“ gegen die „Kommunikationsteilhabe Außenstehender“,[989] die Abwehr von erzwungener Vergemein-

[982] Podlech (1976c, S. 319 ff.). ‘Eine Datenschutzregelung ist nur so gut, wie sie das Problem der Geheimdienste regelt, und das bedeutet, daß alle derzeitigen Regelungen schlecht sind.“ (S. 320).
[983] Podlech (1976c, S. 321). Dabei sei eine Benachrichtigung allein nicht ausreichend.
[984] Podlech (1976c, S. 321).
[985] Podlech (1976c, S. 322).
[986] Siehe Rüpke (1976, S. 19).
[987] Siehe Rüpke (1976, S. 33).
[988] Siehe Rüpke (1976, S. 53).
[989] Siehe Rüpke (1976, S. 85 ff.).

schaftung, also der „Aufzwingung eines Gesprächspartners“,[990] sowie die Abwehr einer „Konfrontation mit Außenstehenden, die sich jedoch das für persönlich-vertraute Partnerschaft erforderliche Vorverständnis einseitig auf dem Umweg über die Kenntnisnahme der Sozialisations- und Lebensgeschichte des Betroffenen verschafft haben“, also die Abwehr einer „Usurpation einer Partnerstellung“.[991] Seine ganze Konstruktion ist aber nur vorgeschoben, denn dahinter verbirgt sich nichts weiter als eine verklausulierte Sphärentheorie, nur eben eine, die weniger auf abrupten als vielmehr auf fließenden Übergängen zwischen den Sphären basiert: Wenn die Kommunikation weniger „persönlich“ sei, könne sie auch weniger geschützt sein.[992] Und aus seiner Fehlwiedergabe der spezifischen Bezugnahme der frühen Datenschutzdiskussion auf die Rollentheorie[993] – nicht Goffman, sondern Luhmann und damit Parsons – sowie der Fehlwiedergabe der Rollentheorie selbst – Rollenspiel wird von keiner Rollentheorie als „rigide“ unterstellt – folgt, dass er nicht verstehen kann, dass sein Ansatz selbst gegenüber den strukturalistisch-rollentheoretisch begründeten Ansätzen noch zu kurz greift: Mit der Rollentheorie in Verbindung mit dem Informationsbegriff der Semiotik kann jede Rolle, jede Kommunikation, jeder Kontext und jeder Zweck und deren jeweile Eigenlogiken, Normen und Erwartungen gegen die Übergriffigkeit jeder anderen Rolle, jeder anderen Kommunikation, jedes anderen Kontexts und jedes anderen Zwecks als schutzbedürftig markiert werden.

In seiner Ende 1975 abgeschlossenen, von Spiros Simitis und Walter Schmidt begutachteten und 1977 veröffentlichten Dissertation „Zielfunktionen des Datenschutzes“[994] versucht Otto Mallmann die „allen Überlegungen über angemessene Schutzinstrumente notwendig vorgeschaltete Frage, [...] was also Datenschutz gegen welche Gefahren schützen soll“,[995] zu beantworten, denn:

> „Meist begnügt man sich mit pauschalen Hinweisen auf die Privatsphäre, die es zu schützen gelte. Damit wird ein Konsens vorgetäuscht, der in Wahrheit gar nicht besteht.“[996]

Gleichwohl bezieht sich auch Mallmann nachfolgend auf nicht mehr als die Privatsphäre, indem er in seiner Arbeit unterscheiden will zwischen „dem individuellen Interesse am Schutz der Privatsphäre und demjenigen an der Gewährleistung korrekter Information“.[997]

Mit Verweis auf vorwiegend amerikanische Literatur sieht Mallmann einen „Strukturwandel personenbezogener Datenverarbeitung“, der sich einerseits in der „Erhöhung der gespeicherten Datenmenge“, andererseits in der „vermehrte[n] Datenzirkulation“ begründet.[998] Darauf aufbauend versucht er, Privatsphäre zu bestimmen.[999] Dabei folgt er weitgehend den Vorarbeiten von Westin, Shils und Habermas und beschreibt „Privatheit“, die er mit „Privatsphäre“ gleichsetzt, als „zentrale Kategorie liberalen Gesellschaftsverständnisses“, als Bereich, „in dem [der einzelne] frei, d. h. ohne staatliche Reglementierung über seine materiellen und immateriellen Ressourcen

[990] Siehe Rüpke (1976, S. 95 ff.).
[991] Siehe Rüpke (1976, S. 115 f.).
[992] Siehe Rüpke (1976, S. 122 ff.).
[993] Siehe Rüpke (1976, S. 136 ff.).
[994] Mallmann (1977).
[995] Mallmann (1977, S. 9).
[996] Mallmann (1977, S. 9).
[997] Mallmann (1977, S. 10).
[998] Mallmann (1977, S. 12 ff.). Er verweist dabei vor allem auf Westin und Baker (1972), Martin und Norman (1972), U.S. Department of Health, Education, and Welfare (1973), aber auch Westin (1967), Rule (1973) und Dammann et al. (1974).
[999] Mallmann (1977, S. 16 ff.).

verfügen kann."[1000] Dazu gehören nach Mallmann „Geheimnisse", „Intimsphäre", „Respektabilität" und „Individualismus".[1001] Für die USA und die Bundesrepublik beschreibt er dann die Verrechtlichung des Privatsphärenschutzes.[1002] Das allgemeine Persönlichkeitsrecht diene, so Mallmann, neben dem Schutz der Ehre vor allem der Abschirmung der Privatsphäre.[1003]

Anschließend beschäftigt sich Mallmann mit der Begründung eines „informationsbezogenen, nicht allein auf eine räumliche Schutzzone abstellenden Privatheitsbegriffs".[1004] Den für das Recht wegen der Relativität der Privatsphäre gewählten Anknüpfungspunkt des personenbezogenen Datums lehnt er dabei genauso ab wie das dem Recht auf informationelle Selbstbestimmung zugrunde liegende Modell uneingeschränkter Privatautonomie,[1005] denn er unterstellt, dass „[e]chte Möglichkeiten informationeller Selbstbestimmung [...] nur in der Interaktion zwischen machtmäßig annähernd gleichgewichtigen Partnern" bestehen.[1006] Darüber hinaus erklärt er es für kaum realisierbar, dem einzelnen die „Möglichkeit einer aktiven Steuerung der Verbreitung ihn betreffender Informationen zu ermöglichen", und im übrigen wegen der damit einhergehenden „Überbetonung individueller Interessen" auch nicht für wünschenswert.[1007] Stattdessen übernimmt er die Definition Müllers und will „Privatsphäre" definieren als „ein je nach der individuellen und gesellschaftlichen Interessenkonstellation unterschiedlicher Bereich von Nichtinformation über Individuen".[1008] Allerdings:

> „Die Entscheidung über Information oder Nichtinformation, d. h. über die jeweilige Zulässigkeit von Informationsverarbeitung, kann dabei weder prinzipiell vom Betroffenen – wohin aber die Konzeption informationeller Selbstbestimmungsrechte zielt – noch allein von den Informationsinteressenten – wie es weitgehend der bisherigen Praxis entspricht – getroffen werden. Vielmehr ist es Aufgabe der Rechtsordnung, auf Grund einer Untersuchung der jeweiligen Konfliktsituationen die Beziehungen zwischen dem einzelnen und staatlichen und privatwirtschaftlichen Informationssystemen vorzustrukturieren. [...]
>
> Konturen gewinnt Privatheit erst auf Grund einer Analyse, die festzustellen hat, welche individuellen Interessen sie gegen welche Gefahren schützen soll."[1009]

Diese Analyse will Mallmann derart durchführen, dass er – ohne dabei darauf zu verweisen, dass er hier einfach Westin[1010] folgt – „die Funktionen [untersucht], die Privatsphäre erfüllt, und die Konsequenzen, die sich für diese Funktionen jeweils aus einer verstärkten Transparenz des Individuums durch Datenverbundsysteme ergeben."[1011]

Zu Beginn fragt Mallmann nach der Verwendbarkeit der soziologischen Rollentheorie für die Analyse des Datenschutzproblems.[1012] Nach dem interaktionistischen Rollenkonzept, das er der

[1000] Mallmann (1977, S. 17 f.).
[1001] Mallmann (1977, S. 16 ff.).
[1002] Mallmann (1977, S. 21 ff.).
[1003] Mallmann (1977, S. 24).
[1004] Mallmann (1977, S. 25).
[1005] Mallmann (1977, S. 26 ff.). Mallmann stellt hier fest, dass es sich bei der informationellen Selbstbestimmung um eine simple Übernahme der Ausführungen von Westin (1967) und Fried (1968) handelt, siehe S. 27.
[1006] Mallmann (1977, S. 28).
[1007] Mallmann (1977, S. 29).
[1008] Mallmann (1977, S. 30).
[1009] Mallmann (1977, S. 30).
[1010] Westin (1967).
[1011] Mallmann (1977, S. 35).
[1012] Mallmann (1977, S. 36 ff.).

Analyse zugrunde legt, bleibt nur dann Raum für eine notwendige Rolleninterpretation durch das Individuum, „wenn die Interaktionspartner nicht schon erschöpfend informiert sind.“[1013] Privatheit sei somit „Voraussetzung für ein flexibles, distanziertes Verhältnis zur Rolle.“[1014] Mit Hilfe von „Computerdossiers“ würde jedoch die Rolle fixiert, Verhaltenserwartungen würden rigider und wenn die einzelne „den Grad der Informiertheit des anderen“ nicht mehr abschätzen könne, würde die „beim Rollenspiel bewußt oder unbewußt vorgenommene Kalkulation der Wirkung eigenen Verhaltens auf das Gegenüber [...] entscheidend erschwert“.[1015] Mallmann behauptet, dass sich die Rollentheorie zwar eigne, „einige[] Konsequenzen von Datenverbundsystemen auf Individuum und Gesellschaft“ zu beschreiben, greife jedoch zu kurz, denn sie könne „[n]icht alle Gefahren [...] adäquat beschreiben.“[1016] Für diese Behauptung gibt er jedoch keine Begründung an, sondern verweist nur – quasi als Begründungsersatz – darauf, dass „die Rollentheorie deshalb meist nur in Verbindung mit anderen Ansätzen verwendet“ werde.[1017] Auch als „Instrument rechtlicher Regelung, als Mittel zur Steuerung von Informationsflüssen“ sei die Rollentheorie zwar durchaus brauchbar, jedoch „für sich allein genommen nicht ausreich[end].“[1018] „Hier können rollentheoretische Überlegungen nicht die Analyse des jeweiligen Verwendungszusammenhangs der Informationen und die Abwägung der beteiligten Interessen ersetzen.“[1019] Insgesamt entsteht hier der Eindruck einer unzulässigen Vermischung der Frage nach der Funktion von Datenschutz für den Schutz des Individuums mit der Frage nach dem Ansatz für eine rechtliche Regelung.

Zweitens – und auch hier folgt Mallmann den Ausführungen Westins – reflektiert er die „unterschiedlichen Intensitätsgrade“ „intersubjektiver Beziehungen“ unter dem Titel „Intimität und Distanz“.[1020] Insoweit er sich auch hier in Goffmans Fußstapfen bewegt, behandelt er im Kern den inneren Ablauf des Rollenspiels – trotz der vorgenommenen Trennung im Aufbau des Textes. Auch Mallmanns dritter Abschnitt zu den Funktionen „der Privatsphäre“ – „Identität und Selbsteinschätzung“[1021] – bezieht sich auf die rollentheoretische Beschreibung und Erklärung dieses inneren Rollenspiels, in diesem Fall auf den Prozess, in dem Individuen „sich selbst [...] definieren, sich eine Identität [...] schaffen.“[1022] Viertens versucht Mallmann, das Verhältnis von „Privatheit“ und „Individualautonomie“ zu klären.[1023] Auch hierzu bedient er sich wieder ausführlich bei rollentheoretischen Ansätzen und Erklärungen und bleibt dabei eine Begründung für seine getrennte Betrachtung schuldig. In diesem Abschnitt beschäftigt er sich vergleichswei-

[1013] Mallmann (1977, S. 38).
[1014] Mallmann (1977, S. 39).
[1015] Mallmann (1977, S. 39 f.).
[1016] Mallmann (1977, S. 44).
[1017] Mallmann (1977, S. 40, Fn. 164) mit Verweis auf Westin (1967, S. 34 f.).
[1018] Mallmann (1977, S. 44).
[1019] Mallmann (1977, S. 44). Mallmanns Ausführungen überzeugen nicht. Entweder sind sie trivial: Natürlich ersetzen rollentheoretische Überlegungen nicht schon die Abwägung. Oder sie sind schlicht falsch: Die Frage des Verwendungszusammenhangs kann sehr wohl rollentheoretisch analysiert werden, siehe etwa Dammann (1973) oder Müller (1975b). Mallmanns Behauptung, Rollentheorie blende Interessen aus, entspricht weder Goffmans Ausführungen zur Rollentheorie, auf die er sich explizit bezieht, noch entspricht sie der Konzeption auf der Basis von Parsons, Merton und Luhmann: Interessen sind dort gerade ein notwendiger Bestandteil des Rollenkonzepts.
[1020] Mallmann (1977, S. 45 ff.).
[1021] Mallmann (1977, S. 47 ff.).
[1022] Mallmann (1977, S. 48).
[1023] Mallmann (1977, S. 52 ff.).

se ausschweifend mit den Folgen von „Überwachungsmechanismen“, die er als „Apathie und Anpassung“ identifiziert.[1024]

Im Ergebnis will Mallmann feststellen, dass „Privatheit [...] eine Reihe essentieller Funktionen für die Gesellschaft und den einzelnen“ erfülle, und dass gerade ein Menschenbild, dass das Individuum als „gemeinschaftsbezogen und -gebunden ansieht“, „zugleich eine differenzierte gesellschaftliche Informationsstruktur“ bedinge.[1025] Aufgabe des Datenschutzes sei es, so Mallmann, „Privatheit angesichts der von den modernen Informationstechnologien, aber auch von perfektionierten manuellen Systemen ausgehenden Gefahren zu gewährleisten“[1026] – Datenschutz sei also nichts weiter als Privatheitsschutz.[1027]

Als zweite große Zielfunktion des Datenschutzes identifiziert Mallmann die „Gewährleistung von Richtigkeit und Vollständigkeit der Informationen“.[1028] In seiner Begründung für Korrektheit und Vollständigkeit als Schutzobjekt geht er über die im Rahmen der Datensicherungsdiskussion adressierten Aspekte hinaus und verweist auf die spezifische Rolle von Informationen für die Entscheidungsproduktion.[1029] „Entscheidung ist essentiell Informationsverarbeitung“, wobei maßgeblich für die Entscheidung „jeweils vom Entscheider herangezogene Informationen über den betroffenen einzelnen“ seien.[1030] Und diese Informationen könnten, so Mallmann, „wenn sie entsprechend aufbereitet [sind], die folgende menschliche Entscheidung präjudizieren.“[1031] Gleichzeitig schwänden die „oft ohnehin bescheidenen Partizipations- und Einwirkungschancen des Betroffenen“, während gleichzeitig nicht über diesen entschieden würde, „sondern über sein Datenprofil“.[1032] Entscheidung sei dabei Produkt eines im voraus defininierten und formalisierten Entscheidungsprozesses, der den Einwirkungsmöglichkeiten der Betroffenen entzogen wird und zugleich – zwar nur scheinbar, aber dafür sehr effektiv – nicht mehr der Verantwortlichkeit der Entscheiderinnen unterliegt.[1033] Datenschutz soll, so Mallmann, „in diesem Zusammenhang [...] für die Betroffenen undurchsichtige Informations- und Organisationsstrukturen transparent [...] machen“.[1034]

[1024] Mallmann (1977, S. 55 ff.). Diese Folgendiskussion hätte auch an jedem anderen Ort im Text stehen können, etwa direkt nach der Betrachtung der Rollentheorie oder im Anschluss an den Abschnitt zur Identitätsbildung. Wahrscheinlich wäre es am passendsten gewesen, diese Diskussion als eigenen Abschnitt hinter den beschriebenen vier Funktionen der „Privatheit“ einzuordnen. Allerdings hätte Mallmann dann auch auffallen können, dass sich sein gesamter Abschnitt um die Rollentheorie dreht, und damit aufdecken können, dass seine zu Beginn des Abschnitts geäußerte Kritik an der Geeignetheit der Rollentheorie für die Analyse des Datenschutzproblems nur bedingt haltbar ist.

[1025] Mallmann (1977, S. 67 f.).

[1026] Mallmann (1977, S. 68).

[1027] Mallmann kann hier – wie viele andere auch – nicht erklären, warum „dies Ding“ dann nicht einfach „Privatheitsschutz“ heißen sollte oder historisch so genannt wurde.

[1028] Mallmann (1977, S. 70 ff.).

[1029] Stefan Drackert, der die Bedeutung von Mallmanns Arbeit für die Datenschutzdiskussion weit überschätzt – nicht nur ist sie erst 1977 und damit nach Abschluss des Gesetzgebungsverfahrens erschienen, sondern ihr erster Teil stellt auch im wesentlichen eine Wiederholung der Ausführungen Westins dar, mit der sich die Diskussion zu diesem Zeitpunkt schon kritisch auseinandergesetzt und die sie bereits überwunden hatte –, ignoriert diesen Aspekt vollständig, siehe Drackert (2014, S. 265 ff.).

[1030] Mallmann (1977, S. 71).

[1031] Mallmann (1977, S. 72).

[1032] Mallmann (1977, S. 73).

[1033] Mallmann (1977, S. 73 f.).

[1034] Mallmann (1977, S. 74). Hier zeigt sich eines der Probleme des Mallmannschen Ansatzes: Indem er sich ausschließlich auf den Schutz der Privatsphäre konzentriert, muss er „[p]artizipationsfeindliche Entscheidungsprozesse“, die „keine Verletzung der Privatsphäre [...] bedeuten“, ausklammern (Fn. 17, S. 75), oder zugespitzter: Entscheidungen über Menschen in vermachteten Informationsbeziehungen unterfallen nach seinem Verständnis dem Datenschutz nur dann, wenn sie auf der Basis von Informationen getroffen werden, die „der Privatsphäre

Insgesamt verschenkt Mallmann – von einigen wenigen Ausführungen im Abschnitt zur Korrektheit und Vollständigkeit von Informationen abgesehen – alle Möglichkeiten, in seiner Problemanalyse über den damaligen Stand der Debatte hinauszugehen – es handelt sich im Grunde um eine etwas erweiterte Übersetzung der Arbeit Westins, ergänzt um eine Fallstudie zu Kreditinformationssystemen.

Ende März 1977 fand in Hamburg das von Klaus Brunnstein organisierte Werkstattgespräch „Gesellschaftliche Auswirkungen großer Informationssysteme aus der Sicht verschiedener Disziplinen“ statt, auf dem Hansjürgen Garstka einen wegweisenden, jedoch nur sehr selten wieder aufgegriffenen Vorschlag für die verfassungsrechtliche, insbesondere grundrechtliche Einordnung der Informationsverarbeitung vorstellte: Er schlug vor, „den durch die Grundrechte geschützten Verhaltensraum auf die Informationen über diesen Verhaltensraum auszudehnen“,[1035] d. h. die informationelle Dimension der Grundrechte in den Bereich des Grundrechtsschutzes aufzunehmen und sie so bereichsspezifisch – eben *grundrechts*bereichsspezifisch – zu konkretisieren.[1036]

Kurz nach dem Inkrafttreten des Bundesdatenschutzgesetzes 1978 erschien die für lange Zeit einzige umfassende Arbeit zur Implementierung von Datenschutz- und Datensicherungsmaßnahmen in Informationssysteme am Beispiel eines medizinischen „Informationssystems für Niedergelassene Ärzte“ (INA), die zugleich methodische Fragen des Verfahrens der Implementierung behandelte.[1037] Die Untersuchung entstand bereits 1974, wurde jedoch für die Veröffentlichung überarbeitet, auch im Hinblick auf das erlassene Bundesdatenschutzgesetz, auch wenn dieses nur eine „defiziente Teilmenge sinnvoller Datenschutzvorkehrungen“ mitbrachte.[1038] Ausgangspunkt für die Arbeit von Wilhelm Steinmüller, Leonhard Ermer und Wolfgang Schimmel ist die Feststellung, das Automation eine „formalisierungsbedingte Beseitigung von Handlungsspielräumen zwecks Rationalisierung, Leistungsvermehrung und Leistungserweiterung“ bedeute, und Informationsautomation zusätzlich eine „radikal erhöhte Transparenz (und damit Manipulation) sozialer Systeme zugunsten derjenigen, die über diese Informationssysteme zu Verfügungen berechtigt sind.“[1039] Daraus folge, dass die Einbeziehung vorbestehender rechtlicher Schutzmechanismen in technische Abläufe „unter den Bedingungen maschinisierter Systeme neu realisiert werden“ müsse.[1040]

> „[S]oziale Freiheit ist nunmehr nur noch möglich, wenn sie von vornherein in die Konstruktion der Informationssysteme eingeplant, auch mit den Mitteln der modernen Daten- und Kommunikationstechnologien technisch und organisatorisch abgesichert und schließlich in ihrem sozialen Umfeld rechtlich verankert und gewährleistet wird.“[1041]

Oder deutlicher als strukturalistisches Prinzip:

zuzurechnen sind“ (ebd.). Eine Reflexion über die Frage, ob es hier überhaupt einen objektiven Unterschied zwischen diesen beiden Situationen gibt, findet nicht statt, genauso wenig wie Mallmann problematisiert, inwieweit ein solcher Unterschied subjektiv überhaupt bedeutungsvoll sein kann.

[1035] Siehe Garstka (1977).

[1036] Siehe zu diesem Ansatz auch Gallwas (1979) sowie – viel später und ohne Bezugnahme auf die Vorarbeiten – Albers (2005).

[1037] Steinmüller et al. (1978).

[1038] Steinmüller et al. (1978, S. X).

[1039] Steinmüller et al. (1978, S. 2).

[1040] Steinmüller et al. (1978, S. 2).

[1041] Steinmüller et al. (1978, S. 2). Der „Betroffenenschutz“ müsse dabei „als zur Wirtschaftlichkeit und Flexibilität komplementäres Konstruktionsprinzip“ mit einbezogen werden, Steinmüller et al. (1978, S. 14, Fn. 1).

> „[Es kann] nur noch darum gehen, durch optimale Ausnützung der informationstechnischen und rechtlichen Möglichkeiten *in die Informationssysteme Freiheitsspielräume neu zu implementieren* [...]."[1042]

Datenschutz sei dabei keine „Frage von Einzelmaßnahmen, erst recht nicht von lediglich technischen Vorkehrungen, sondern [eine Frage] der Optimierung der gesamten Systemorganisation im Hinblick auf übergeordnete Zwecke".[1043] Die Formulierung einer geeigneten und angemessenen Datenschutzkonzeption mache dabei „wegen der ständig notwendig werdenden sprachlichen und sachlichen Grenzüberschreitung einen sehr erheblichen interdisziplinären Verständigungsaufwand erforderlich [...], namentlich was den Übergang von technischer Beschreibung zu organisatorischer Strukturierung und normativer Bewertung betrifft."[1044]

Das für die Untersuchung gewählte Beispiel ist ein „riskantes" Informationssystem. Riskante Informationssysteme seien dadurch charakterisiert, dass „eines oder mehrere ihrer Elemente besondere Gefahren für abgebildete Betroffene bergen".[1045] Solche Elemente können etwa sein: „Daten" – dabei sagen die Autoren aber an anderer Stelle zurecht: „Gefährlich sind nicht die Daten, sondern der Benutzer – und der Interessent."[1046] –, „Programme"[1047] und „Umweltrelationen", vor allem „bei »multifunktionalen« Systemen, die sehr verschiedenartigen Interessen dienen oder zu besonders mächtigen oder unkontrollierten Teilsystemen der Gesellschaft in Beziehung stehen".[1048] Gestaltungsziele seien dann die Minimierung möglicher Gefahrenquellen, die Erzeugung von Transparenz und damit Kontrollierbarkeit der Systeme für Betroffene und Benutzerinnen sowie einerseits die Isolation des riskanten Systems von seiner Umwelt und andererseits dessen Verbindung mit dem Umsystem über „verantwortete Koppelungen".[1049] Erst die Isolation der Systeme, deren Zuschneidung auf definierte Informationszwecke und die technische, rechtliche, organisatorische und personelle Absicherung dieser Isolation ermögliche es, „innerhalb der Systeme die Datenverarbeitung relativ unbelastet von Restriktionen" zuzulassen, um damit zugleich hohe Effizienz wie einen hohen Schutz sicherzustellen.[1050]

Für die Übersetzung von rechtlichen Anforderungen in Gestaltungskriterien für Informationssysteme legen die Autoren zuerst die Annahmen über Datenverarbeitung und Datenschutz offen, die der Datenschutzdiskussion – und gerade auch der Datenschutz*rechts*diskussion – zugrunde gelegt wurden und werden, um darauf aufbauen erstens „unzureichende Datenschutzauffassungen zurückzuweisen" und zweitens ihren eigenen Lösungsansatz zu skizzieren.[1051] Datenschutz sei „Kehrseite der Datenverarbeitung" und „im Kern umfassende Informationskontrolle im Interesse und unter Beteiligung" der Betroffenen durch „Normierung der Datenströme und -operationen (»Datenverkehrskontrolle« durch »Programmkontrolle«) sowie organisierte Transparenz des Systems".[1052] Datenschutz sei dabei ein Organisationsproblem und „kein primär technisches Problem", es sei „die organisatorische Antwort auf die durch die spezifische Leistung von Informationssystemen entstehenden spezifischen Gefahren."[1053] Für die im Informationssystem abgebil-

[1042] Steinmüller et al. (1978, S. 90), Hervorhebungen im Original.
[1043] Steinmüller et al. (1978, S. 13).
[1044] Steinmüller et al. (1978, S. 12).
[1045] Steinmüller et al. (1978, S. 193).
[1046] Steinmüller et al. (1978, S. 85).
[1047] Dieses Problem wird heute oft verkürzt als „Algorithmenproblem" bezeichnet. Siehe instruktiv Schinzel (2017).
[1048] Steinmüller et al. (1978, S. 193).
[1049] Steinmüller et al. (1978, S. 194).
[1050] Steinmüller et al. (1978, S. 194).
[1051] Steinmüller et al. (1978, S. 71 ff.).
[1052] Steinmüller et al. (1978, S. 72 f.).
[1053] Steinmüller et al. (1978, S. 76 f.).

deten Betroffenen entstehe durch ihre Abbildung als Modelle und deren quasi unbeschränkte Nutzbarkeit zugunsten des „Systemherrn“ ein „Herrschaftsproblem“, das Hauptgegenstand der Datenschutzdiskussion sei.[1054] Dabei gehe die stärkste Gefährdung der Betroffenen – „entgegen vielfacher Auffassung“,[1055] auch heute noch – keineswegs von illegitimen Informationsinteressentinnen aus, sondern von legitimen Interessentinnen.[1056] Zu den von den Autoren als unzureichend identifizierten Ansätzen gehören der Schutz der „Privatsphäre“,[1057] das Schutzgut „personenbezogene Daten“ als Versuch der Überwindung des beschriebenen „Privatsphäre“-Problems,[1058] genauso wie das Konzept der „sensitiven Daten“[1059] oder auch die „Verrechtlichung des Datenverkehrs“ nebst seiner Varianten „Einwilligungstheorie“ und „Entfremdungstheorie“.[1060]

Der vorgeschlagene Lösungsansatz ergebe sich, so die Autoren, „aus der Kritik der bisherigen Ansätze unter Anwendung informationswissenschaftlicher Gesichtspunkte.“[1061] Der Schutzbereich soll umfassend sein und alle Daten einbeziehen, nicht nur die personenbezogenen, ferner alle Arten von Datenverarbeitung, d. h. manuelle wie automatisierte, „alle Phasen, Formen und Prozeduren der Datenverarbeitung [...], von der ersten Datenerfassung bis zur Löschung.“[1062] Wichtigstes Ziel sei eine „von vornherein kontrollfreundliche Strukturierung“ des Systems.[1063] Dies werde erreicht durch „Programmkontrolle“:

> „Da die Maschinisierung geistiger Funktionen durch die ADV sich in den Algorithmen (Programmen) verkörpert, liegt auch hier der Kern des Schutzes; *Programmkontrolle* ermöglicht die Nachprüfbarkeit aller Datenverarbeitungsprozesse; Datenflüsse werden durch Programme geregelt, sie sind die Verkehrswege der Daten im Informationssystem.“[1064]

Hinzu käme eine „kompetenzorientierte Datenverarbeitung“, die sicherstellen müsse, dass „das Minimum an legitimen Benutzern das legitime Minimum and Informationen verarbeitet und

[1054] Steinmüller et al. (1978, S. 79). Der Ausschluss des „Marktproblems“, das den Ausschluss von Betroffenen von der Nutzung der Systemleistung bezeichnen soll, aus dem Gegenstandsbereich des Datenschutzes, den die Autoren hier vornehmen, widerspricht ihren vorherigen Ausführungen zum Institutionaldatenschutz, siehe S. 74 f., sowie dem Postulat der Beteiligung der Betroffenen, siehe S. 73.

[1055] Steinmüller et al. (1978, S. 80).

[1056] Steinmüller et al. (1978, S. 81).

[1057] Siehe Steinmüller et al. (1978, S. 82 ff.), vor allem wegen seiner Relativität zur jeweiligen Systemnutzerin.

[1058] Siehe Steinmüller et al. (1978, S. 84 f.), denn auch der Personenbezug sei nur relativ, „nämlich bezogen auf die spezifische Leistung, Benutzer- und Interessenstruktur des jeweiligen Informationssystems“ (S. 85). Das ist zwar korrekt, aber immer noch zu kurz gegriffen, weil nur auf die Re-Identifizierbarkeit abstellend, wie noch zu zeigen sein wird, denn es ignoriert völlig, dass Menschen auch an nicht personenbezogenen Informationen „gemessen“, d. h. Entscheidungen über Menschen auf Basis solcher Informationen getroffen werden können.

[1059] Steinmüller et al. (1978, S. 85 f.).

[1060] Steinmüller et al. (1978, S. 86 ff.): Eine vollständige Verrechtlichung scheitere an der Komplexität der Realität (S. 86), das Einwilligungsprinzip opfere langfristigen Schutz und gesellschaftliche Interessen dem „individuelle[n] kurzfristige[n] Wohl“ des Betroffenen (S. 86) Später werden die Autoren deutlicher und schneiden dabei auch das zentrale Problem der Einwilligung an: Eine Patientin „vermag nur nach Rechtsinformatikstudium die Tragweite [ihrer] Zustimmung zu überblicken“, siehe S. 154 – die aus der zunehmenden Arbeitsteilung folgende zunehmende Spezialisierung bei gleichzeitigem relativen Kompetenzverlust in Bereichen außerhalb des Spezialisierungsgebiets muss in der breiten Bevölkerung tendenziell zu abnehmender Fähigkeit zur Abschätzung der individuellen und gesellschaftlichen Folgen moderner Informationsverarbeitung führen, siehe Pohle (2015b), und ermögliche dem „Systemherrn“ die Ausnutzung einer sozialen Machtposition (S. 87), und eine strikte Zweckentfremdungsregel schlösse nicht nur jede Planung und Forschung aus, sondern auch jede „übergreifende Rationalisierung [...] im Bereich der medizinischen Versorgung“ (S. 87 f.).

[1061] Steinmüller et al. (1978, S. 90).

[1062] Steinmüller et al. (1978, S. 90 f.).

[1063] Steinmüller et al. (1978, S. 91).

[1064] Steinmüller et al. (1978, S. 91 f.), Hervorhebung im Original.

weitergibt".[1065] Flankierend müssten die „Möglichkeiten der Datensicherung [...] in den Dienst des Datenschutzes gestellt werden", etwa die eindeutige Zuordenbarkeit von „Daten zu Kompetenzen, Kontexten und Benutzern" und deren Absicherung sowie technische Sicherungen gegen ungenehmigte Programme und Programmänderungen.[1066] Die Phasen seien so zu organisieren, „daß sie auch in ihrer Interaktion transparent bleiben."[1067] Gleiches gelte auch für die Arbeitsteilung zwischen Informationsorganisation und ärztlicher Tätigkeit.[1068] Zur Stabilisierung der Transparenz bedürfe es einer funktionierenden Fremdkontrolle zusätzlich zur informationstechnischen und organisatorischen Festschreibung von „Datenbedarf und Datenverkehr" durch eine unabhängige Instanz, „die diese Fixierung überwacht und die notwendigen Veränderungen legitimiert", mit Sachkunde, fehlendem Eigeninteresse, weisungsfreier Stellung und angemessener Ausstattung.[1069] Die Autoren verpassen in diesem Zusammenhang die Chance, über eine technische Absicherung der Kontroll- und Abwehrrechte der Betroffenen sowie der Kontrollrechte der Aufsichtsorgane zu reflektieren, und verweisen stattdessen nur darauf, dass „eindeutige techische, organisatorische und rechtliche Verantwortungen [dafür] getroffen werden müssen."[1070] Die allgemeinen Ausführungen zum Lösungsansatz werden anschließend in zehn INA-bezogene Datenschutzpostulate überführt,[1071] von denen nur einige sich nicht schon in der vorhergehenden Darstellung wiederfinden, wie etwa die Ausdehnung der Abschottung auf Empfängersysteme, aus dem das Verbot einer Datenweitergabe „ohne Nachweis von für diesen Informationskontext ausreichenden Datenschutzvorkehrungen im und durch das Empfängersysteme" folgt,[1072] oder das Postulat der definierten Struktur – nicht im Sinne einer statischen Festschreibung, sondern zur Erschwerung nicht verantworteter und nicht definierter Änderungen am System.[1073]

Mit dem Ziel einer „möglichst vollständigen Abschottung des Systems nach außen" bei gleichzeitig „optimale[r] Bereitstellung von Informationen für übergeordnete gesundheitspolitische und allgemeine Planungszwecke sowie für die wissenschaftliche Forschung" wird anschließend ein Datenschutzkonzept vorgestellt, das vor allem auf konsequenter Pseudonymisierung aller verarbeiteten Daten – sowohl von Patientinnen wie von Ärztinnen – verbunden mit einer an unterschiedlichen Informationsinteressen ausgerichteten Rollentrennung basiert und sowohl definierte Verantwortlichkeiten schafft und diese personell zuweist als auch ein Kontroll- und Freigabeorgan institutionalisiert, mit dem zugleich die Entwicklungsoffenheit des Systems sichergestellt werden soll.[1074] Die Autoren weisen dabei explizit darauf hin, dass wegen der „Transformierbarkeit der Datenkategorien" die vorgelegte Lösung mittels Pseudonymisierung nur „bei entsprechender Programmkontrolle und Abschottung (und nur dann)" datenschutzkonform sei.[1075] Für kontext- und zweckabhängige Informationen – exemplarisch genannt werden Diagnosen für verschiedene Zwecke wie Überweisungen, Nachweise für Arbeitgeberinnen oder Gerichte – schlagen die Auto-

[1065] Steinmüller et al. (1978, S. 92 f.).
[1066] Steinmüller et al. (1978, S. 93).
[1067] Steinmüller et al. (1978, S. 94).
[1068] Steinmüller et al. (1978, S. 94).
[1069] Steinmüller et al. (1978, S. 94).
[1070] Steinmüller et al. (1978, S. 95). Siehe aber auch S. 132 zur „computerunterstützten Patientenberatung" und zur möglichen Öffnung des „Auskunftssystems" für Patientinnen.
[1071] Steinmüller et al. (1978, S. 96 ff.).
[1072] Steinmüller et al. (1978, S. 99).
[1073] Steinmüller et al. (1978, S. 100).
[1074] Steinmüller et al. (1978, S. 105 ff.).
[1075] Steinmüller et al. (1978, S. 112), siehe auch S. 114.

ren vor, zusammen mit den Informationen den Herkunftskontext zu speichern.[1076] Andererseits wird im Zusammenhang mit der Beschreibung der Programmkontrolle deutlich, welchem (Fehl-)Verständnis die Autoren hinsichtlich von Programmen unterliegen: Sie imaginieren Programme als technische Implementation von (vorher abschließend definierten) „Arbeitsabläufen“ und können (nur) aus diesem Grund für ihr Datenschutzkonzept annehmen, dass „[f]ür Patienten und Arzt gefährliche Datenoperationen [...] nur durch unerlaubte Datenverarbeitung entstehen“ kann, nämlich entweder durch „unerlaubten Gebrauch genehmigter Programme“ oder durch „unerlaubten Gebrauch ungenehmigter Programme“.[1077] Ein besonderer Schwerpunkt in der Darstellung des Datenschutzkonzepts wird auf die „Interessenten“ gelegt, d. h. systemexterne Informationssysteme.[1078] Das Prinzip der Abschottung erfordere eine vollständige Definition aller Schnittstellen des Systems, während jedoch INA als multifunktionales System, das selbst wiederum in ein komplexes System – das Gesundheits- und Sozialwesen mit Versorgung, Vorsorge und Gesundheits- und Sozialpolitik – eingebettet ist, in dem verschiedene widerstreitende Interessen aufeinandertreffen und viele – gerade auch konkurrierende – davon gesetzlich oder vertraglich normiert sind. Die Autoren schlagen daher eine „Interimslösung“ vor, eine dem schwedischen „datalag“ entsprechende „Institutionalisierung von »trial and error«“,[1079] die für INA Erfahrungen mit den Informationsinteressentinnen sammeln, allgemeine Regelungen entwerfen und vorschlagen, „Einzelfallprobleme [...] auf ihren generellen Hintergrund [...] durchdenken und [...] lösen“, Datenschutzmaßnahmen bei Interessentinnen durchsetzen, „Transmitterstelle für legitime externe Datenwünsche und ihre kontrollierte Befriedigung“ sein soll und dabei „wegen ihres geringen Fixierungsgrades *hoch adaptiv*“ sei.[1080] Informationsinteressentinnen müssten dabei gegenüber INA den Nachweis führen, dass sie „nur berechtigte Operationen mit der berechtigten Datenmenge vornehmen“ werden und dass ihre Informationssysteme „eine datenschutzkonforme Organisation“ aufweisen.[1081]

Das in der Untersuchung entwickelte Datensicherungskonzept ist explizit als „datenschutzorientiert“ ausgewiesen, indem unter „Datensicherung“ auch „alle Maßnahmen technischer wie organisatorischer Art zur Realisierung des beabsichtigten Datenschutzes“ verstanden werden sollen.[1082] Die im Datenschutzkonzept problematisierten Verarbeitungen und Verwendungen von Daten, „die das Persönlichkeitsrecht der Betroffenen gefährde[n] oder verletzen“ können, werden mit anderen unberechtigten Verwendungen von Daten, Programmen und Rechenzeit unter dem Begriff „Mißbrauch“ zusammengefasst.[1083] Die Maßnahmen zielen dabei darauf ab, sowohl die Eintrittswahrscheinlichkeit von Gefahrenereignissen zu verringern als den eingetretenen Schaden dabei so gering wie möglich zu halten sowie einen Wiederanlauf des Systems im Schadensfall, eine nachträgliche Revision und die Aufdeckung von Fehlern oder Missbräuchen zu ermöglichen.[1084]

[1076] Steinmüller et al. (1978, S. 113). Nach den Ausführungen auf S. 123 sollen jeweils auch die berechtigten Adressatinnen automatisch mitgespeichert werden, um „pragmatische Korrektheit (Kontexttransparenz)“ zumindest für „das sendende System“ zu erreichen.

[1077] Steinmüller et al. (1978, S. 118), siehe auch S. 117, insbesondere Fn. 2. Dort wird gefordert, dass den Nutzerinnen „nur parameterisierte Methodenaufrufe (Programmaufrufe) zur Verfügung gestellt“ werden dürfen. Wie sehr dieses (enge und inzwischen von der technischen Entwicklung überholte) Verständnis auch das Datenschutzrecht prägte, ist schon gezeigt worden, siehe Pohle (2014b).

[1078] Steinmüller et al. (1978, S. 134 ff.).

[1079] Steinmüller et al. (1978, S. 136 f.).

[1080] Steinmüller et al. (1978, S. 138).

[1081] Steinmüller et al. (1978, S. 140).

[1082] Steinmüller et al. (1978, S. 157 f.).

[1083] Steinmüller et al. (1978, S. 160).

[1084] Steinmüller et al. (1978, S. 160 f.).

Die Arbeit ist in der Forschung weitgehend unbeachtet geblieben, gerade auch in der Informatik. Vor allem wurde sie nie einer grundlegenden Kritik unterzogen. Dies ist umso misslicher, als sich in ihr kondensiert die Annahmen wiederfinden, die in der ersten Phase der Datenschutzdiskussion prägend waren für die Gestaltung des Datenschutzrechts, das bis heute eine starke architektonische Kontinuität gewahrt hat.[1085]

Mit dem Beschluss und dem Inkrafttreten des Bundesdatenschutzgesetzes endete eine Ära – die Ära der intensiven Diskussion über die Beschreibung, Einordnung, Begründung und „Lösung" des Datenschutzproblems als gesellschaftlichem Problem. Stattdessen konzentrierte sich die Diskussion nunmehr in erster Linie auf Anwendungs- und Auslegungsprobleme.[1086] Dabei wird insbesondere die Frage, inwieweit das Bundesdatenschutzgesetz überhaupt eine Lösung des gesellschaftlichen Datenschutzproblems darstellt, weitgehend ausgeklammert. Diese grundlegende Tendenz der Neuverortung der Diskussion zeigt sich auch in den beteiligten Akteurinnen: Die überwiegende Mehrheit wendet sich den Anwendungsproblemen zu und geht in die Praxis, sei es in die entstehenden Datenschutzaufsichtsbehörden oder die anwaltliche Praxis, einige verlagern den Schwerpunkt ihrer Arbeit, etwa hin zur Verwaltungsinformatik, und nur wenige – wie Podlech und Steinmüller – halten die Grundsatzdiskussion am Laufen, nicht zuletzt mit dem Ziel, die im Laufe der 1970er Jahre in der wissenschaftlichen Debatte aufgeworfenen grundsätzlichen Probleme noch datenschutzrechtlich „lösen" zu können, denn das meiste davon wurde vom Gesetzgeber ignoriert.[1087]

Dem umfangreichen Material, das Werner Liedtke seiner rechtssoziologischen Untersuchung des Gesetzgebungsprozesses zum Bundesdatenschutzgesetz analysiert hat, zufolge hat sich die Gesetzgebungsdebatte offensichtlich zwischen 1972 und 1974 von der wissenschaftlichen Debatte entkoppelt – sie wurde einerseits hochgradig selbstreferenziell, andererseits jedoch auch stark beeinflusst von den Interessen von Privatwirtschaft und Verwaltung, deren Lobbies schon damals hervorragenden Zugriff auf den Gesetzgeber sowie die zuarbeitende Ministerialbürokratie hatten.[1088] Allein die Tatsache, dass das von Herbert Auernhammer geleitete Referat im Bundesministerium des Innern Steinmüllers Gutachten „Grundfragen des Datenschutzes" zur Grundlage der Regelungsarchitektur des Bundesdatenschutzgesetzes machte,[1089] verhinderte die völlige Unwissenschaftlichkeit von Problemanalyse und gesetzlicher Regelung als „Lösung" dieses Problems, wie es etwa noch für das erste Hessische Landesdatenschutzgesetz kennzeichnend war.[1090] Dennoch bleibt festzuhalten, dass das BDSG in erster Linie eine gesetzliche Festschreibung der bestehenden vermachteten Informationsordnung, d. h. der „freiheitsbedrohende[n] gesellschaftli-

[1085] Siehe Pohle (2014a).

[1086] Siehe dazu auch Hümmerich und Kniffka (1979), insbesondere S. 1189, die das offensichtlich begrüßen. Der Gegensatz, den die Autoren aufmachen, ist selbst jedoch nur ein innerjuristischer: Die grundsätzliche Diskussion, die nun in den Hintergrund trete, verorten sie vor allem im Bereich des Verfassungsrechts.

[1087] Siehe dazu und zum folgenden die umfassende Abhandlung Liedtke (1980).

[1088] Siehe dazu Liedtke (1980, S. 262 ff., passim). Bezeichnend sind etwa die Äußerungen von Werner Ruckriegel und Joachim Schweinoch, Ziel sei, „daß es die Wirtschaft nicht unnötig belastet" und „die Belastungen für die Wirtschaft im Interesse des Datenschutzes so gering wie möglich zu halten", siehe Liedtke (1980, S. 252, Fn. 330).

[1089] Diese Tatsache ignoriert Liedtke, siehe Liedtke (1980, S. 254), der die „weitreichende Vorentscheidung" des Bundesdatenschutzgesetzes durch den Referentenentwurf allein bei den Autorinnen dieses Entwurfs – darunter Auernhammer, Egon Hölder und Rudolf Schomerus, von denen zwei später wichtige Kommentatoren des BDSG werden sollten – verortet.

[1090] Hinsichtlich der anderen aus dem Kreis der Wissenschaft und aus der Mitte des Parlaments stammenden Gesetzesentwürfe – Interparlamentarische Arbeitsgemeinschaft 1971, Adalbert Podlech 1973, Bundestags-Innenausschuss 1976 – trifft Liedtkes Analyse jedoch zu, siehe insbesondere Liedtke (1980, S. 139 ff.).

che[n] Tendenzen zur absoluten Kontrolle fast aller durch wenige“,[1091] war.[1092] Und selbst wenn das Gesetz eine geeignete Basis zur Adressierung des gesellschaftlichen Datenschutzproblems darstellte, war damit keineswegs sichergestellt, dass nicht durch passende Auslegung der Schutz, den das Gesetz hätte bieten können, unterminiert wurde.[1093] Dennoch sind zumindest einige der offenkundigsten Lücken in späteren Novellierungen, vor allem nach dem Bundesverfassungsgerichtsurteil zur Volkszählung, geschlossen worden.

2.4 Zwischen Kontinuitäten und Umbrüchen

2.4.1 Schwächephase nach den ersten Datenschutzgesetzen

Während die Datenschutzdiskussion in der Bundesrepublik – von Ausnahmen abgesehen – verflachte und verstärkt zur Rechtsdiskussion, und dort vor allem zur Auslegungsdiskussion, mutierte, behielt sie insbesondere in den USA ihre vorherige Breite bei, wahrscheinlich bedingt durch das Fehlen eines allgemeinen Datenschutzgesetzes.

Auf der einen Seite standen dabei sehr eingeschränkte Konzeptionen wie die von Richard A. Posner und George J. Stigler.[1094] Posner definiert „privacy“ einfach als instrumentelles Interesse an Geheimhaltung von Informationen, vor allem „discreditable informationen, often information concerning past or present criminal activity or moral conduct at variance with a person's confessed moral standards“[1095] mit dem vorherrschenden Ziel „to mislead others“.[1096] Unter Verweis das Problem falscher Angaben über Waren im Kaufvertragsrecht[1097] schlussfolgert Posner, dass es „generally no protection for facts about people“ geben sollte.[1098] Gleichwohl – und das ist vor dem Hintergrund von Posners Argumentation zu Ablehnung von *privacy* für Individuen scheinbar überraschend – fordert er „the protection of trade and business secrets by which businessmen exploit their superior knowledge or skills“.[1099] Es ist jedoch nur scheinbar überraschend: Zwar will er mit seinen Arbeiten eine ökonomische Analyse vorlegen, beschränkt sich jedoch zugleich auf „personal rather than business contexts“,[1100] um dann eine rein ökonomisierte Form des instrumentellen *privacy*-Interesses zu unterstellen – „not to desire or value privacy [... in itself] but to use these goods as input in the production of income or some other broad measure of utility or welfare“[1101] –, um dann doch vor allem auf die große Bedeutung zu verweisen, die Informationsverarbeitung im Wirtschaftsbereich habe.[1102] Kurz: Posners „Analyse“ ist verkürzt,[1103] geprägt von seiner Ergebnisorientierung, Folge seiner unbegründeten Annahmen und zugleich in

[1091] Liedtke (1980, S. 257).
[1092] Siehe auch Bieber (1978).
[1093] Siehe etwa die Auflösung des Erforderlichkeitsprinzips und seine Ersetzung durch die „Wünsche“ nach Datenvermeidung und Datensparsamkeit, Pohle (2014b, Rn. 14, vor allem Fn. 25., Rn. 28 und Fn. 37), oder die Umdefinition einer „Datenschutz-by-Design“-Regelung in eine Datensicherheitsregelung, Pohle (2015a).
[1094] Siehe Posner (1978a), Posner (1978b), Posner (1981) und Stigler (1980). Siehe auch die Kritik von Hirshleifer (1980).
[1095] Posner (1978a, S. 21 f.), Posner (1978b, S. 399).
[1096] Posner (1978a, S. 22).
[1097] Siehe Posner (1978b, S. 399 f.) oder „fraud in the sale of goods“, S. 401.
[1098] Siehe Posner (1978b, S. 404).
[1099] Posner (1978b, S. 404).
[1100] Siehe Posner (1978a, S. 19), Posner (1978b, S. 393).
[1101] Posner (1978b, S. 394).
[1102] Siehe etwa Posner (1978b, S. 394 f., 400, passim).
[1103] Seine Ausführungen legen nahe, dass er sich *privacy rights* gar nicht anders vorstellen kann denn als *property rights*, siehe etwa Posner (1978b, S. 399).

sich widersprüchlich – das einzig verwunderliche ist, dass Posner bis heute als einer der Ahnen der wirtschaftswissenschaftlichen Beschäftigung mit *privacy* gilt. Wie Posner imaginiert auch Stigler jeden Datenverarbeiter als Person, vor allem wenn es darum geht, die negativen „Folgen" von *privacy* zu beschreiben,[1104] während er sonst ganz selbstverständlich davon spricht, dass es sich in erster Linie um Organisationen wie den Staat oder Unternehmen handelt.[1105] Und auch Stigler kann nur in Kategorien von property rights und ownership denken.[1106]

Auf der anderen Seite stehen die – wenn auch nicht unbedingt besseren, so doch nicht nur beschränkt ökonomistisch argumentierenden – allgemeineren *privacy*-Theorien und -Konzepte. Ein großer Teil davon betracht auch nur interpersonale Verhältnisse oder basiert auf zugrunde gelegten Theorien, deren Gegenstandsbereich nur interpersonale Verhältnisse umfasst. William H. Foddy und William R. J. Finighan versuchen, *privacy* aus der soziologischen Theorie des symbolischen Interaktionismus heraus zu konzeptionalisieren.[1107] Sie bauen dabei sowohl Versatzstücke von Goffman wie von Altman ein, ohne sich gleichzeitig explizit zu Goffmans Rollentheorie zu bekennen – die selbst aus dem symbolischen Interaktionismus abgeleitet wurde –, oder Altmans Konzept einer „boundary" des Selbst übernehmen zu wollen. Während Müller mit Parsons und Merton das Agieren in einer durch Rollenspiel geprägten Welt als Bezugspunkt nimmt, fokussieren die Autoren auf die Identitätskonstruktion und -aufrechterhaltung „within a specific role relationship",[1108] zitieren zugleich jedoch Müller und Kuhlmann zum Problem des rollengrenzenübergreifenden Informationsflusses.[1109]

Mit dem Ziel, Forderungen nach *privacy* sinnvoll zu kategorisieren und zu gruppieren sowie ihren rechtlichen Schutz zu begründen, versucht Ruth Gavison, zwischen einem neutralen Konzept von *privacy* und dem Wert von *privacy* zu unterscheiden.[1110] Sie unterscheidet zwischen dem Status – ob es sich bei *privacy* um eine Situation, ein Recht, einen Anspruch, eine Form von Kontrolle oder einen Wert handelt – und den Eigenschaften – ob *privacy* sich auf Informationen, Autonomy, Identität, physischem Zugang bezieht[1111] – und entscheidet sich dann, *privacy* als „a situation of an individual vis-à-vis others, or as a condition of life" zu definieren[1112] und zu charakterisieren als „our accessibility to others" – physisch, informationell und als Objekt fremder Aufmerksamkeit.[1113] Die Funktionen von *privacy* seien „the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society."[1114] Perfekte *privacy* habe, wer „completely inaccessible to others" sei: „no one has any information about *X*, no one pays attention to *X*, and no one has physical access to *X*."[1115] Auf dieser Basis definiert sie dann das Konzept des Verlusts von *privacy*: „as others obtain information about an

[1104] Siehe etwa „a public official" Stigler (1980, S. 623) oder „other persons" (S. 628). Siehe zu seinen Annahmen S. 641 ff.

[1105] Siehe der Verweis auf Banken, das Bureau of the Census und „other governmental agencies", Stigler (1980, S. 624).

[1106] Siehe Stigler (1980, S. 625 und 625 ff., passim).

[1107] Siehe Foddy und Finighan (1980). Die auf George Herbert Mead gründende Handlungstheorie des symbolischen Interaktionismus beschreibt unter anderem, wie sich Menschen im symbolisch vermittelten Prozess der Interaktion mit anderen Menschen eine Identität bilden und aufrechterhalten, siehe Mead (1934).

[1108] Siehe ihre *privacy*-Definition Foddy und Finighan (1980, S. 6).

[1109] Siehe Foddy und Finighan (1980, S. 9) mit Verweis auf Müller und Kuhlmann (1972).

[1110] Gavison (1980). An diesem Beispiel nachträglicher Systembildung – im deutschen Recht: Dogmatik – zeigen sich alle Probleme dieses Vorgehens.

[1111] Siehe Gavison (1980, S. 424).

[1112] Gavison (1980, S. 425).

[1113] Siehe Gavison (1980, S. 423).

[1114] Gavison (1980, S. 423), siehe auch S. 442.

[1115] Gavison (1980, S. 428). *Privacy* sei, so Gavison, das Gegenteil zu Interaktion, S. 440.

individual, pay attention to him, or gain access to him.“[1116] Indem sie „accountability“ und „interference“ explizit aus dem Gegenstandsbereich ihrer Betrachtung ausschließt,[1117] kann sie *privacy* als Komplex aus den an sich distinkten und unabhängigen, jedoch verbundenen Konzepten „secrecy“, „anonymity“ und „solitude“ konstruieren.[1118] Ihre weiteren Ausführungen folgen dann dieser Selbstbeschränkung, die dabei an einigen Stellen noch verstärkt wird, und sind zugleich deren Ergebnis: So schließt sie etwa kategorisch aus, dass es zu einem *privacy*-Verlust kommen könne, wenn die Informationen nicht geheim seien.[1119] Anschließend folgen seitenlange Ausführungen über die Funktionen von *privacy*, die Gavison aus allen möglichen Quellen zusammenträgt, vor allem aus anderen *privacy*-Theorien. Aus der Tatsache, dass sie so viele Konzepte und Theorien aufzählen kann, schlussfolgert sie dann – ohne jede Begründung, warum dafür die Aufzählung der Theorien und Konzepte ausreichen soll –, dass „some privacy is necessary“ für Menschen, „may [...] contribute to a more pluralistic society“und sogar „privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen“.[1120] Abschließend kommt Gavison – nachdem sie noch einmal darauf verwiesen hat, woher *privacy*-Verletzungen *nur* kommen können: von „journalists, doctors, detectives, policemen, and therapists“, also Personen[1121] – zum Ergebnis, dass das Recht zwar eigentlich das falsche Mittel sei, um *privacy* zu schützen, aber „a commitment to privacy as a legal value may help to raise awareness of its importance and thus deter reckless invasions.“[1122]

Als reines Geheimhaltungsinteresse definiert auch W. A. Parent *privacy*, jedoch noch eingeschränkt auf „undocumented“ personenbezogene Informationen.[1123] Dazu grenzt sie ihr Konzept von anderen, wohl eher zufällig ausgewählten Konzepten ab – vom „right to be let alone“, von „autonomy or control over significant personal matters“ sowie von der „limitation on access to the self“ –, indem sie alle diese Konzepte erst sehr eng versteht, d. h. sie nimmt die Kurzfassung einfach wörtlich, und dann „widerlegt“.[1124] Sie geht diesen Weg offensichtlich, weil sie das Ziel verfolgt, „the mistaking of privacy for a part of liberty“ zu verhindern[1125] und *privacy* von *solitude*, „the condition of being physically alone“, abzugrenzen.[1126] Wo sie dann über die Funktionen von *privacy* „reflektiert“, vermischt sie dann die Konzepte doch wieder: *Privacy* ver-

[1116] Gavison (1980, S. 428).
[1117] Siehe Gavison (1980, S. 429).
[1118] Siehe Gavison (1980, S. 428 f.).
[1119] Siehe Gavison (1980, S. 429): Die drei angeführten Fälle lassen sich, etwa unter Rückgriff auf Kohler (1880) oder Warren und Brandeis (1890) oder auf Müller und Kuhlmann (1972) sehr wohl als Verletzungen der *privacy* klassifizieren, aber Gavison schließt das aus, weil ihr „Filter“, den sie an der Stelle plötzlich offenlegt, das ausfiltert: „In none of these cases is there any intrusion, trespass, falsification, appropriation, or exposure of the individual to direct observation.“ Gavison unterlässt es hier, eine Begründung für die Beschränkung auf diese – wahrscheinlich von Prosser übernommenen – Verletzungshandlungen vorzunehmen. Gleichzeitig wird deutlich, dass ihr Konzept selbst widersprüchlich ist: Einerseits soll es eine *privacy*-Verletzung sein, wenn Informationen über Individuen anderen bekannt werden (S. 428), andererseits stelle es keine Verletzung dar, wenn diese Informationen in einer „unbenutzten Datenbank“ liegen (S. 429, Fn. 27) – aber wie sind die da wohl hineingekommen? Ähnlich stellt sich die Lage dar, wenn Gavison versucht, Bloustein zu widerlegen: „Having to beg or sell one's body in order to survive are serious affronts to dignity, but do not appear to involve loss of privacy“, so Gavison (S. 438), während gleichzeitig beide Handlungen offensichtlich unter „physical access“ fallen – was wäre denn mehr physischer Zugang zu einem Menschen als Sex mit ihr?
[1120] Siehe Gavison (1980, S. 455).
[1121] Siehe Gavison (1980, S. 470).
[1122] Gavison (1980, S. 471).
[1123] Siehe Parent (1983).
[1124] Siehe Parent (1983, S. 271 ff.).
[1125] Siehe Parent (1983, S. 273).
[1126] Siehe Parent (1983, S. 275).

hindere die Ausübung von Macht über Personen auf der Basis von „sensitive personal knowledge about us“[1127] – ein klarer und von der Autorin unreflektierter Freiheitsbezug –, *privacy* schütze Scham in „a society where individuals are generally intolerant of life styles, habits, and ways of thinking that differ significantly from their own“[1128] und *privacy* – Geheimhaltung von „certain facts about us“ – sei ein Selbstzweck in der „liberal ideology“.[1129] Sie schlussfolgert, *privacy* schütze „the distinctively liberal, moral principle of respect for persons“[1130] und sei „a moral value for persons who also prize freedom and individuality.“[1131] Parent versucht dann, Kriterien zu entwickeln, um gerechtfertigte von ungerechtfertigten *privacy invasions* unterscheiden zu können und wiederholt dabei die damals schon allgemein anerkannten, wenn auch auf niedrigem Niveau: legitimer Zweck, Relevanz der Informationen für den Zweck, mit den am wenigsten eingreifenden Mitteln, mit prozeduralen Schutzmaßnahmen und Datensicherheit.[1132]

Alle diese Konzeptionen gehen davon aus, dass nur Menschen mögliche Angreiferinnen sein können – Organisationen werden schlicht ignoriert.[1133] Im Grunde handelt es sich um nichts anderes als Befindlichkeiten, was hier jeweils geschützt werden soll – oder wie bei Posner, abgeschafft werden soll.

Auf einer dritten Seite stehen Arbeiten, die das Problem der modernen Informationsverarbeitung aus strukturalistischer – oder zumindest aus gesamtgesellschaftlicher – Sicht untersuchen. Sie stellen jedoch eine Minderheit dar, können damit jedoch zugleich Aspekte in den Blick nehmen, die den individualistischen und interpersonalen Theorien verschlossen bleiben müssen, wie etwa die Verstetigung spezifischer gesellschaftlicher Machtstrukturen im Zuge der weltweiten Vernetzung von informationstechnischen Systemen[1134] oder das Problem von Verantwortungszuweisung und Verantwortlichkeit, Aufsicht und Kontrolle bei komplexen Informationssystemen, die selbst wieder in komplexe soziale und politische Umgebungen eingebettet sind.[1135]

[1127] Parent (1983, S. 276).
[1128] Parent (1983, S. 276).
[1129] Siehe Parent (1983, S. 276 f.).
[1130] Parent (1983, S. 277).
[1131] Parent (1983, S. 278).
[1132] Siehe Parent (1983, S. 280).
[1133] Am deutlichsten hat Posner das gezeigt, als er 2005 behauptete, es könne sich nicht um *privacy*-Verletzungen handeln, solange nur Computer personenbezogene Informationen verarbeiten würden: „The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.“, Posner (2005).
[1134] Siehe dazu etwa Schiller (1978), der nicht nur zu Beginn fragt: „Is what's good for IBM good for the world“ und darauf antwortet: „The answer may depend on the kind of world that's envisaged.“, sondern auch J. Hugh Faulkner, den damaligen kanadischen Minister für Wissenschaft und Technik, mit der Warnung zitiert, dass in Zukunft der Zugriff auf lebenswichtige Informationen von den Entscheidungen von Interessengruppen abhängen könnte, die außerhalb jeder Kontrolle situierten – eine Problembeschreibung, die auch sehr direkt auf Googles oder Facebooks heutige Rolle bei der globalen Kontrolle von Informationen, etwa zu politischen Entscheidungen, zutrifft.
[1135] Siehe dazu etwa Laudon (1980): Solche Informationssysteme dürften nur errichtet werden, wenn Verantwortlichkeiten klar geregelt seien, eine unabhängige Aufsicht existiere und deren Datenqualität sichergestellt werden, andernfalls seien deren „social and legal consequences [...] unpredictable“ (S. 56) und damit diese Systeme gesellschaftlich inakzeptabel. Siehe dazu auch Laudons spätere Arbeit zur Frage, inwieweit Organisationen überhaupt rechtsstaatlich und fair – „due process“ – über Individuen Entscheidungen treffen könne, wenn die Qualität der Informationen, die diese Organisationen gespeichert haben, nicht sichergestellt werden kann, am Beispiel von Datenbanken mit Strafeinträgen bei Strafverfolgungsbehörden in den USA – die Qualität

Die zweite große Untersuchung zur Frühphase der *privacy*- und Datenschutzdiskussion und deren Verwirklichung im Recht stammt von James Rule, Douglas McAdam, Linda Stearns und David Uglow.[1136] Im Gegensatz zu Liedtke analysieren sie allerdings weniger die Aushandlungsprozesse, die zur Verrechtlichung geführt haben, als vielmehr die Problemanalysen und die „Lösungen" für die Probleme im Recht. Sie gehen dabei von einer sehr breiten *privacy*-Definition – „the restriction of others' access to information about oneself"[1137] – und einer ebenso breiten *surveillance*-Definition – „the systematic monitoring of personal data"[1138] – aus. Der Zweck von „surveillance" sei „social control", „any means of influence by which a person or an organization seeks to render other people's behavior or circumstances more predictable and more acceptable."[1139] Aus dieser Konstruktion der Begriffe ergibt sich offenkundig, dass es keine „surveillance" geben kann, die nicht zugleich eine *privacy*-verletzung darstellt.[1140] Die Beschreibung der gesellschaftlichen Realität erinnert – trotz der gegenteiligen Behauptung der Autorinnen, alle anderen in der Welt würden nur durch die amerikanische Diskussion beeinflusst sein und dabei „heavily" Alan Westin folgen[1141] – stark an die deutsche Datenschutzdebatte der 1970er: Moderne (S. 25), spezialisierte (S. 26) und rationale (S. 27) Bürokratien (S. 28) – formale Organisationen (S. 27), Maschinen, „whose overall output is made predictable through the predictable interrelations of each part within them" (S. 28) – in hochgradig arbeitsteiligen (S. 26) Gesellschaften – „an »organized« world" (S. 29) –, deren Folge die zunehmende gegenseitige Abhängigkeit der sozialen Teilsysteme sei (S. 26), die mit Individuen nur noch in deren hochgradig beschränkten Rollen interagieren (S. 27), die die Organisationen den Menschen zusammen mit den zugehörigen Rollenerwartungen aufnötigen (S. 28), benötigten Informationen über diese Menschen, um unter Unsicherheitsbedingungen (S. 44) Entscheidungen über sie zu treffen (S. 49):[1142]

> "It is no exaggeration to describe modern organizations as engaged in the »production« of authoritative decisions about people, or to characterize personal information as the »raw material« for this production.„[1143]

Auch für die Rolle der Technik im Gebrauch durch Organisationen und die Beschreibung der Folgen sind die Parallelen unübersehbar:

---

sei mies, so Laudon, die Daten seien „fundamentally incomplete, ambiguous, and inaccurate", siehe Laudon (1986a, S. 10).

[1136] Rule et al. (1980).

[1137] Rule et al. (1980, S. 23). Sie definieren zwei Unterfälle: „*aesthetic* privacy" als Selbstzweck und „*strategic* privacy" als Mittel für einen anderen Zweck, S. 22.

[1138] Rule et al. (1980, S. 47).

[1139] Rule et al. (1980, S. 47). Beide Termini – „surveillance" und „social control" – seien in einem neutralen Sinne gemeint und wertfrei, so die Autorinnen, ibid. Rule wird darauf aufbauend später den Begriff „mass surveillance" prägen: „the monitoring by large organizations of large numbers of ordinary people", Rule (1983, S. 176).

[1140] Dieses Problem haben die Surveillance Studies geerbt, die sich unter anderem auf Rules Arbeiten beziehen – natürlich neben dem Übervater Foucault –: Mit dem *surveillance*-Begriff wird eine allgemeine (gesellschaftliche) Praxis von organisierten Sozialsystemen in modernen Gesellschaften als gesellschaftliches Problem aufgeworfen, das dann mit dem *privacy*-Begriff wieder individualisiert wird.

[1141] Siehe Rule et al. (1980, S. 112).

[1142] Diese Beschreibung kommt fast ohne Quellenangaben aus, aber schon in seinem erstem Werk zu diesem Themenbereich, Rule (1973), auf das immer wieder verwiesen wird, bezieht sich Rule vor allem auf Arbeiten Talcott Parsons und seiner Schülerinnen. Und Luhmanns Frühwerk, das in der deutschen Debatte breit rezipiert wurde, ist eine – aus Luhmanns Sicht – Weiterentwicklung der Theorie Parsons'. Die Ähnlichkeit zwischen Rule et al.'s Beschreibung und der in der deutschen Datenschutzdebatte überrascht daher nicht.

[1143] Rule et al. (1980, S. 49).

> „[P]ersonal-data systems [...] confer unprecedented power upon bureaucracies to pursue their ends efficiently; but the existence of these powers poses risks which must at some point be counted unacceptable.“[1144]

Allein in der Selbstbeschränkung auf personenbezogene Informationen – die Autorinnen unterscheiden nicht zwischen „data“ und „information“ – findet sich ein Unterschied zu den Ergebnissen der deutschen Debatte im Jahrzehnt zuvor.

Im Rahmen der Arbeit werden anschließend die „Antworten“ auf das *privacy*-Problem, also sowohl die Problembeschreibungen wie die „Lösungen“ und deren Umsetzung im (US-amerikanischen) Recht, analysiert – „Privacy and Freedom“ (1967), „The Assault on Privacy“ (1971), der Fair Credit Reporting Act (1970), „Records, Computers, and the Rights of Citizens“ (1973), der Privacy Act of 1974, der „Personal Privacy in an Information Society“ (1977) sowie „Databanks in a Free Society: Computers, Record-Keeping and Privacy“ (1972).[1145] Die Autorinnen kritisieren, dass alle Studien sich vor allem auf die vielzähligen „abuses“ und „abusive practices“ konzentrieren würden und dabei und damit die großen Fragen ausklammerten:[1146]

> „How much surveillance do we really want? How far into previously private areas of life ought these systems to extend? At what point does even just, efficient monitoring of private affairs become excessive?“[1147]

Entsprechend würden dann auch die „Lösungen“ aussehen: Surveillance sei akzeptabel, wenn die Informationen korrekt, vollständig und aktuell seien, wenn *surveillance* und Entscheidungen auf der Basis von „openly promulgated rules of »due process«“ getroffen würden, wenn Organisationen nur die für legitime Zwecke erforderlichen Informationen erheben und nutzen würden und wenn es umfassende Betroffenenrechte gebe.[1148] Organisationen, die sich an diese Regeln hielten, könnten dann „claim to protect the privacy“ der Betroffenen:

> „From the standpoint of surveillance organizations, this is a most opportune interpretation of »privacy protection.«“[1149]

Als Gegenmodell schlagen die Autorinnen Datensparsamkeit vor, müssen aber zugleich eingestehen, dass diese Alternative bislang ignoriert worden sei. Stattdessen würden alle Beteiligten dem Effizienzkriterium huldigen und damit auch die *privacy*-Verteidigerinnen in eine Falle laufen:

> „The beguiling thing about the emergent reform consensus is that it seems to offer something for everybody. For the general public, beset by demands for personal data, it offers assurance that »privacy« is being »protected,« even as organizations amass more and more personal information. Yet such protection is to be achieved without disturbing any of the conveniences associated in the public mind with organizational surveillance. From the institutional point of view, the picture is even brighter. In exchange for acceptance of procedural reforms, surveillance organizations achieve legitimacy and public support for their activities.

[1144] Rule et al. (1980, S. 9).
[1145] Siehe Westin (1967), Miller (1971), U.S. Department of Health, Education, and Welfare (1973), Privacy Protection Study Commission (1977), Westin und Baker (1972). Die Arbeiten und Gesetze werden in dieser Reihenfolge, nicht in der Reihenfolge ihrer Entstehung oder ihres Erscheinens, analysiert.
[1146] Siehe Rule et al. (1980, S. 70 f.).
[1147] Rule et al. (1980, S. 71).
[1148] Siehe Rule et al. (1980, S. 71).
[1149] Rule et al. (1980, S. 71).

> Perhaps most important of all, acceptance of the »efficiency criterion« undercuts potential public opposition to more and more sweeping surveillance: It becomes impossible to object to any surveillance practice, provided that data are used efficiently for the ends of some established organization—and provided this use occurs with fairness, accuracy, thoroughness, due process, and provision for participation by the individual concerned. Having agreed to play the game, those speaking for the interests of the public can hardly complain as the stakes are raised. And these stakes, in terms of the shifting balance of power between mass publics and centralized organizations, may well rise without limit. Thus the official interpretation of privacy protection actually encourages the growth of surveillance and the erosion of personal privacy.“[1150]

Damit aber – und das darf nicht übersehen werden – laufen die Autorinnen in ihre eigene Falle: Das, was sie hier als *privacy*-Verletzungen beschreiben und aus fundamentalen Gründen – „keeping private spheres private“[1151] – rundheraus ablehnen, ist das Ergebnis ihrer eigenen – und nur ihrer eigenen – *privacy*-Definition. Hier liegt dann auch der entscheidende Unterschied zur Datenschutzdebatte: Die Datenschutzdebatte setzt auf dem Rechtsstaat und den dort historisch erkämpften Freiheits- und Beteiligungsrechten sowie seinen freiheits- und beteiligungssichernden Organisationsprinzipien auf und entwickelt sie weiter, damit sie auch unter den Bedingungen moderner Informationsverarbeitung gesichert werden können, während Rule und Kolleginnen – etwas überraschend vor dem Hintergrund, dass Rule ein Anhänger Parsons' ist – schlicht einen alten überkommenen *Zustand* – den Zustand der Vormoderne – aufrechterhalten wollen und nicht nur die *Möglichkeit der gesellschaftlichen Aushandlung* des gesellschaftlichen erwünschten Zustands der gesellschaftlichen Machtverteilung.[1152] Das räumen sie selbst ein und formulieren dementsprechend als Kritik an der Forderung nach rechtsstaatlicher Einhegung der Informationsmacht von Organisationen:

> „Certainly such guarantees, when they work, may establish limits to organizations' power. But such procedural limitations can scarcely recreate the distribution of power that existed before these centralized data systems grew up.“[1153]

Dabei böte ihre Analyse eine sinnvolle Basis für die Frage nach der gesellschaftlichen Aushandelbarkeit gesellschaftlicher Machtverhältnisse und den Bedingungen ihrer Möglichkeiten in von Organisationen geprägten modernen Gesellschaften. Ihr Vorschlag für eine Operationalisierung ihrer Forderung nach Zurückdrehung der gesellschaftlichen Machtverschiebungen zugunsten von Organisationen setzt jedenfalls an der richtigen Stelle an, obwohl die Verbindung zur Frage der Unsicherheitsabsorption[1154] nicht gezogen wird:

> „Organizations collect personal information to make decisions about people. Better data means more accurate discriminations among the people with whom organizations must deal—hence better decisions, from the viewpoint of the organization. [...]

[1150] Rule et al. (1980, S. 72).
[1151] Rule et al. (1980, S. 71).
[1152] Die Beschreibung des Umfangs und der Tiefe moderner Informationsverarbeitung, die die Autorinnen liefern – „Certainly no area of human life is inherently too private to attract the application of bureaucratic surveillance. Indeed, the most sensitive and »personal« aspects of life are often most associated with the social uncertainties which make systematic monitoring and control attractive.“ (S. 136) –, erinnert stark an den Ausgangspunkt der deutschen Datenschutzdebatte.
[1153] Rule et al. (1980, S. 81).
[1154] Siehe Rule et al. (1980, S. 44).

> If organizations were not expected to make such highly refined distinctions between people, the need for rigorous data collection would be greatly eased. *The alternative to endless erosion of personal privacy through increased surveillance is for organizations to relax the discriminations which they seek to make in their treatment of people.* [...] We propose a reallocation of resources toward less discriminatory, less »information-intensive« ways of dealing with people.“[1155]

Zwei damit zusammenhängende Aspekte verdienen noch Aufmerksamkeit: Während Rule et al. einem Argument, das relational mit dem Begriff „besser“ operiert, entgegenhalten, die Frage sei, „what range of alternatives have been taken into account in making the implied comparison?“,[1156] stellen sie sich nicht die gleiche Frage, wenn es darum geht, ob die von ihnen beschriebene Realität organisierter Informationsverarbeitung nicht die gleichen Konsequenzen in Fällen hat, in denen keine personenbezogenen Informationen verarbeitet werden. Und zweitens: Sie werfen am Ende ihrer Arbeit das Problem der Zentralisierung mit seiner Folge der Schaffung großer – im Sinne Brunnsteins Werkstattgespräche – Informationssysteme auf, wenn auch im Vergleich zur restlichen Diskussion eher oberflächlich, und schlagen dazu vor, besser auf kleine, „weiche“ und verteilte Systeme zu setzen, die im Schadensfall zumindest den Bereich des Schadens begrenzen könnten.[1157]

Die Auseinandersetzung darüber, welchen (individuellen und gesellschaftlichen) Zielen Vorrang vor welchen anderen eingeräumt werden soll und welchen Anforderungen moderne Informationsverarbeitung und -nutzung genügen muss, wurde auch über Landesgrenzen hinweg geführt. Ein von Simon Nora und Alain Minc erstellter Bericht an den französischen Staatspräsidenten zur „L'informatisation de la Société“ von 1978, der im gleichen Jahr in großer Auflage als Buchausgabe erschien und in Frankreich auf große Resonanz gestoßen war, wurde im darauffolgenden Jahr von der Gesellschaft für Mathematik und Datenverarbeitung in der Bundesrepublik publiziert, wenn auch ohne die Anlagen, die im Original in vier Anlagenbänden erschienen und die in der deutschen Ausgabe nur in einer Kurzfassung abgedruckt wurden.[1158] Der Bericht adressiert die gesamte Breite der als „Informatisierung“ bezeichneten „zunehmende[n] Durchdringung der Gesellschaft und ihrer Teilsysteme und der Organisationen mit Informationstechnologien“:[1159] vom Verhältnis zwischen zentralen und dezentralen Organisationseinheiten des Staates, über das Verhältnis Staat–Bürgerin und Fragen der Bürgerinnenbeteiligung, Freiheitsrechte, die Arbeitswelt, die öffentliche Verwaltung bis hin zur Wirtschaftspolitik.[1160] Die zwei größten Mängel, die dem Bericht in der öffentlichen Debatte vorgeworfen wurden, seien nach Kalbhen die Ignoranz gegenüber dem allgemeinen Problem der zunehmenden Verdatung sowie die Fixierung von Nora und Minc auf „große, kanalisierte und staatlich geregelte »Telematik«“.[1161] Ein wesentlicher Teil der Veränderungen, die von der Informatisierung ausgelöst würden, betreffe die gesellschaftlichen Kräfteverhältnisse. Dabei sei die Informationsverarbeitung ein „beinahe vollkommen flexibles

[1155] Rule et al. (1980, S. 154). Hervorhebung im Original.
[1156] Rule et al. (1980, S. 177).
[1157] Siehe Rule et al. (1980, S. 186).
[1158] Nora und Minc (1979).
[1159] Nora und Minc (1979, S. 15).
[1160] Siehe die Übersicht in der Einleitung des Herausgebers Nora und Minc (1979, S. 17 f.).
[1161] Nora und Minc (1979, S. 22). Wie auch von Rule et al. gefordert, solle nicht großen Systemen der Vorzug gegeben werden, sondern kleinen. Der Neologismus *télématique* beschreibt die wachsende Verflechtung von Informationsverarbeitung und Telekommunikation, die Konvergenz von Computern und Übertragungsnetzen, siehe Nora und Minc (1979, S. 15, 35 ff.), mit der Folge, dass das „Informatiknetz“ dem Stromnetz immer ähnlicher werde, Nora und Minc (1979, S. 45).

Werkzeug“, das „sich ohne große Mühe jeder Art von Machtverhältnissen anpassen“ könne.[1162] Dieses „neutrale“ Werkzeug könne wie in der traditionellen Datenverarbeitung „hierarchisch organisiert, isoliert und zentralistisch“ sein oder „»entflochten« und verteilt, dezentralisiert oder autonom“ werden: „dies ist eine Frage von Entscheidungen.“[1163] Als die Gefahren für die Freiheitsrechte, die nach Meinung der Autoren „oft sogar überschätzt“ würden, „weil Computer und Dateien einen Symbolcharakter angenommen haben, der alle allergischen Reaktionen gegenüber der Modernität auf sich vereinigt“, werden die „eventuellen Indiskretionsmöglichkeiten“ identifiziert, denen „die Vorteile der Informatik, ihre Effizienz und ihre Vereinfachungsmöglichkeiten“ gegenübergestellt werden, die einfach „akzeptiert“ werden müssten, auch weil „höhere soziale Transparenz und eine bessere Kenntnis der kollektiven und individuellen Lagen nicht immer von Übel sind.“[1164] Stattdessen liege die Gefahr „anderswo, nämlich in der Labilität der ganzen Gesellschaft“, die vor allem aus den in zentralisierten Systemen zunehmend geschaffenen „neuralgische[n] Stellen“ (Single Points of Failure) resultiere.[1165] Den Abschluss des Berichts bilden zwei Hypothesen; eine kreist um die Konflikte, die alle Elemente des sozialen Lebens erfassen würden – Sprache und Herrschaft, Wissen und Macht –, während die andere um die Sozialisierung von Informationen im Sinne einer partizipativen Informationsgesellschaft.[1166] Insbesondere die Ausführungen zur zweiten Hypothese sind geprägt von einer – auch sonst im Bericht oft durchscheinenden – Ideologie eines gesellschaftlichen Gleichgewichts, die durch eine durchgängig absolut unkritische Bezugnahme auf Effizienz ergänzt wird.

In einer von Frits Hondius und Paul Sieghart herausgegebenen Sonderausgabe der Zeitschrift „Computer Networks“ wurde der Brückenschlag zwischen den Disziplinen versucht, um den „computer people“ das Problem von „data protection“ nahezubringen, das sich, so die Herausgeber im Editorial etwas beschränkt, insbesondere auf „the handling of personal information“ beziehe: „When someone handles information about someone else, that other person will often be affected in some way as a result – frequently to his advantage, but sometimes to his detriment.“[1167] Die Beiträge in der Sonderausgabe, die sich nicht nur auf eine Wiedergabe der Rechtslage beschränken oder gleich ganz über IT-Sicherheit schreiben,[1168] lassen sich klar in zwei Gruppen trennen: Die eine Seite will unter allen Umständen einen „free flow of information“ oder auch einen „free international flow of information“ aufrechterhalten und dafür den

[1162] Nora und Minc (1979, S. 63 f.).

[1163] Siehe Nora und Minc (1979, S. 65). Siehe dazu auch die in die gleiche Richtung argumentierende Untersuchung von Kling und Iacono (1989). Dabei ist jedoch zu beachten, dass nicht wenige von Nora und Mincs Ausführungen im Detail durchaus unsinnig sind, siehe etwa die Behauptung, die „klassische Datenverarbeitung blieb unternehmensintern“ und „veränderte nicht die Beziehungen des Unternehmens zu den Konkurrenten, Partnern, Vertragshändlern oder Zulieferern“ (S. 68).

[1164] Siehe Nora und Minc (1979, S. 73 f.).

[1165] Siehe Nora und Minc (1979, S. 74).

[1166] Siehe Nora und Minc (1979, S. 119 ff.).

[1167] Hondius und Sieghart (1979, S. 147). Hier ist die beschränkte Problemsicht deutlich sichtbar: Aus „that other person“ lässt sich klar schließen, dass die Herausgeber davon ausgingen, dass die Informationen von einer Person verarbeitet werden, nicht von einer Organisation.

[1168] Siehe etwa Stadlen (1979) für den ersten Fall oder Rooms und Dexter (1979) für den zweiten. Außen vor gelassen ist hier Masuda (1979), der auf der Basis einer Periodisierung, die dem japanischen „plan for information society“ zugrunde liegt, für die dort als vierte Periode bezeichnete Zeit von 1980 bis 2000 „vorhersagt“, die computergestützte Informationsverarbeitung dort sei „private person based“ und führe zu einer grundsätzlichen Änderung des gesellschaftlichen Umgangs mit Informationen, nämlich zu einer *post-privacy*-Gesellschaft, in der „all citizens [...] make personal data files in information utilities as open as possible“, Masuda (1979, S. 169). Siehe zur Kritik an solchen naiven Vorstellungen schon Warner und Stone (1970, S. 179) oder Dammann (1974b, S. 281 ff.).

Schutz der Betroffenen möglichst weit einschränken.[1169] Dabei gehen sie offensichtlich davon aus, dass sie die Interessen der (gerade auch privaten) Datenverarbeiter mit den Interessen der Gesellschaft gleichsetzen können, mit denen dann die Interessen der Individuen ausbalanciert werden müssen.[1170] Auf der anderen Seite steht Wilhelm Steinmüller:[1171] Er beginnt damit, dass er aufzeigt, dass eine juristische Beschäftigung mit den durch die Computerisierung der Gesellschaft erzeugten „Probleme“ erst beginnen kann, wenn der Charakter von Informationsverarbeitung und „computer networks“ sowie die devon erzeugten sozialen Probleme klar seien, denn die durch das Recht zu lösenden Probleme in diesem Bereich seien nur eine Teilmenge der sozialen Probleme insgesamt, und gleichzeitig würde die rechtliche „Lösung“ selbst wieder neue Probleme erzeugen, die dann wiederum gelöst werden müssten.[1172] Zur Überbrückung der disziplinären Grenzen schlägt er dann die Nutzung einer gemeinsamen Sprache vor – der Sprache der Systemtheorie – und die Prognostizierung künftiger Entwicklungen im Bereich der Computernetze.[1173] Zwei Entwicklungslinien seien absehbar: Einerseits würden die Netzwerke immer allgemeiner – „the immense capability of computer technology to assimilate other information technologies is a historically unique phenomenon“ –, andererseits gebe es jedoch auch eine Entwicklung hin zu immer spezialisierteren Systemen, und in beiden Fällen eine Tendenz zur umfassenden Vernetzung der Systeme.[1174] In der Folge werden „comprehensive possibilities of the capture, storage, and transfer of all data about all socially relevant facts and systems [...] technically feasible through computer networks“,[1175] die von drei Tendenzen gekennzeichnet seien: der Bevorzugung einfacher Lösungen gegenüber der Nichtverdatung „with the result that important contextual issues are excluded – to the disadvantage of the data subject“, die Verwendung unterkomplexer Modelle, die mit höheren gesellschaftlichen Risiken verbunden seien, und eine einseitig auf wirtschaftlichen Nutzen ausgerichtete Netzgestaltung.[1176] Aus der modelltheoretischen Interpretation der Information folge letztendlich, dass Informationen, Informationssysteme und -netzwerke Machtmittel seien, „ideal means for the planning, guidance and control of social processes“,[1177] mit Auswirkungen auf mindestens drei Ebenen: Auf der Ebene des individuellen Arbeitsprozesses führe die Informationsautomation zu einer erhöhten Kontrolle der abhängig Beschäftigten in der Informationsverarbeitung selbst, auf der Ebene der Organisationen führe sie zu zunehmender Rationalisierung und Zentralisierung mit der Ausschaltung von Zwischeninstanzen und den damit verbundenen Mitbestimmungsrechten und auf der gesell-

[1169] Siehe vor allem die Beiträge von Kirby (1979), Parsons (1979) und Golsong (1979). Entweder der „free flow of information“ stellt immer eine Verletzung von *privacy* oder Datenschutz dar, dann ist das Aufrechterhalten dieses freien Informationsflusses nicht vereinbar mit dem Schutz von *privacy* und Datenschutz. Oder es gibt keinen grundsätzlichen Gegensatz zwischen dem „free flow of information“ auf der einen und *privacy* und Datenschutz auf der anderen Seite, dann müssten beide aber auch nicht zum Ausgleich gebracht werden. Hier ist offensichtlich, dass die Autorinnen klar das erste annehmen und dann das Ziel verfolgen, *privacy* und Datenschutz zugunsten des „free flow of information“ zu beschränken. Deutlich wird hier auch, dass der „free flow of information“ als Selbstzweck angesehen wird und ausschließlich „free“ sein soll, nicht etwa „legitimate“ oder gar „necessary“.

[1170] Siehe etwa Golsong (1979, S. 216).

[1171] Siehe Steinmüller (1979c).

[1172] Siehe Steinmüller (1979c, S. 187). Oder direkter: „[T]he subject of information science and computer science is the description and explanation of information systems, that of social scientists the discussion of the social consequences which arise from them, and that of the lawyer to shape and evaluate those consequences.“ (S. 188).

[1173] Siehe Steinmüller (1979c, S. 189) mit Verweis auf Georg Klaus' „Wörterbuch der Kybernetik“ (1969).

[1174] Siehe Steinmüller (1979c, S. 190).

[1175] Steinmüller (1979c, S. 191).

[1176] Siehe Steinmüller (1979c, S. 192).

[1177] Steinmüller (1979c, S. 193).

schaftlichen Ebene erzeuge sie die Unterwerfung der Bürgerinnen mit ihren Rechten unter die öffentlichen und privaten Organisationen sowie Verwerfungen im gesellschaftlichen Machtgefüge.[1178] Diese Probleme würden dann in vernetzten Systemen weiter verstärkt bis hin zum Fehlen jeder Möglichkeit zur Einflussnahme auf Entscheidungen und deren Kontrolle durch Betroffene, Mitbestimmungsinstitutionen oder Aufsichtsorgane und bei Möglichkeiten zur Flucht der Informationssysteme aus Hochschutz- in Niedrigschutzländer bis zum Ausschluss jeder Aussicht auf eine erfolgversprechende Gegenstrategie aller Betroffenen. Und auf internationaler Ebene gebe es sogar Folgen im Verhältnis zwischen Staaten, wenn die Informationsverteilung durch die Machtbedingungen diktiert werde.[1179] Da ab einer bestimmten Größenordnung alle sozialen Probleme immer auch rechtliche werden würden, müsse das Recht alle vorbeschriebenen Probleme adressieren:[1180] Neben Arbeitnehmerinnenschutz und Mitbestimmungsfragen stünde dabei aus rechtlicher Sicht ein weitgefasster Datenschutz im Vordergrund „to counter the threats to the public and private freedom of action of the citizen“ sowie von Gruppen und gesellschaftlichen Institutionen wie Parteien oder Gewerkschaften, zu dem auch ein Recht auf Informationszugang für Bürgerinnen gegen den Staat gehöre.[1181] Abschließend fordert Steinmüller, dass Systeme grundsätzlich „human-sized“ sein sollen.[1182]

Einen solchen breiten Ansatz bei der Analyse von Netzwerken verfolgte auch die „Interdisziplinäre Arbeitsgruppe Kabelkommunikation Berlin“, die zusammen mit dem Institut für Zukunftsforschung Berlin im September 1978 ein Kolloquium zu „Zweiweg-Kabelfernsehen und Datenschutz“ durchführte und die Ergebnisse in einem Tagungsband publizierte.[1183] Der Leiter der Arbeitsgruppe, Klaus Dette, gab nicht nur eine Einführung in das Kolloquium, sondern auch einen Überblick über die wesentlichen Ergebnisse der Diskussion:[1184] 1) Das Netz sollte Anonymität garantieren, jedenfalls gegenüber Diensteanbietern. 2) Empirische Nutzungsforschung sollte beschränkt werden auf eine repräsentative Auswahl freiwilliger Teilnehmerinnen. 3) Zwei Datenschutzdefinitionen stünden unvereinbar nebeneinander – eine enge („Verhinderung des Mißbrauchs personenbezogener Daten“) und eine weite („Gesamtheit der Maßnahmen zur Ermöglichung und Erhaltung sozialer Verhaltensräume für Individuen und Gruppen unter den Bedingungen moderner Informations- und Kommunikationssysteme“). 4) „Unwidersprochen blieb allerdings der kritische Einwand, daß weder private noch öffentliche Träger künftiger Kommunikationssysteme in der Lage sein werden, einmal gespeicherte Persönlichkeitsprofile gegen Unbefugte hinreichend abzusichern.“ 5) In absehbarer Zeit werde es technisch möglich sein, „Art, Zeitpunkt und Inhalt jeder technisch vermittelten Kommunikation zu archivieren“, daher bedürfe es „im Interesse der Benutzer eine[r] allgemeine[n] Reduzierung der Speicherung personenbezogener Informationen“, und es müssten nicht nur explizite Persönlichkeitsprofile verhindert werden, sondern auch implizite – „Teilnehmer- und Interaktionsdaten, die im Gesamtsystem verteilt sind“. 6) Der Schutz des Fernmeldegeheimnisses allein reiche nicht aus, vor allem vor dem Hintergrund der „sogenannten Abhörgesetze“, und bedürfe daher flankierender spezialgesetzlicher Regelungen. 7) Sowohl Betroffene wie Vertreterinnen „wirtschaftlich und po-

[1178] Siehe Steinmüller (1979c, S. 193 f.).
[1179] Siehe Steinmüller (1979c, S. 195).
[1180] Siehe Steinmüller (1979c, S. 195 ff.).
[1181] Siehe Steinmüller (1979c, S. 196).
[1182] Siehe Steinmüller (1979c, S. 197).
[1183] Siehe Dette et al. (1979). „Zweiweg-Kabelfernsehen“ ist eine Unterkategorie von „Breitbandkommunikation“ und zugleich die „Bildschirmtext“ ermöglichende Technologie, Bildschirmtext ist jedoch – wie Wilhelm Steinmüller Wolfgang Coy nach dessen Bericht mit Hilfe einer hochmittelalterlichen, aus der Scholastik stammenden Methode überzeugend erklärte – ein Computernetzwerk.
[1184] Siehe dazu und zum folgenden Dette (1979).

litisch schwacher Gruppen“ seien stärker zu beteiligen, sowohl bei der Gestaltung wie bei der Kontrolle, etwa im Rundfunkrat. 8) Nutzerinnen würden zugleich zu Produzentinnen. Das datenschutzrechtliche Medienprivileg dürfe nicht auf „Interaktionsdaten“ ausgedehnt werden. 9) Es bedürfe einer intensiveren Zusammenarbeit zwischen Datenschützerinnen, Technikerinnen und Politikerinnen für den Entwurf „wirksamer Datenschutzmaßnahmen und die ständige Gewährleistung des Datenschutzes“. 10) Es bedürfe spezialgesetzlicher Regelungen für zukünftige technische Kommunikationsmedien. Und Datenschutz müsse „integraler Bestandteil des Systementwurfs hochkomplexer Kommunikations- und Informationssysteme“ sein. 11) Die Planung von Datenschutzmaßnahmen müssten auf den vorgesehenen Endausbau abgestimmt werden. Ziel sei eine „kontrollfreundliche und bürgernahe Gestaltung technischer Kommunikations- und Informationssysteme“.

In den Diskussionen zu den Kolloquiumsbeiträgen wurden auch bereits Themen angesprochen, für die teilweise erst sehr viel später die passenden technischen Bedingungen zur Verfügung standen. Dazu gehörte etwa das „Fernwirken und Fernmessen“,[1185] das später als TEMEX von der Deutschen Bundespost wenig erfolgreich umgesetzt wurde[1186] und im Grunde ein Vorläufer heutiger Vernetzungen im Smart Grid ist. Auch Rolf Kreibichs Ausführungen zur „grundlegende[n] Ungleichheit der Datenempfänger, die es praktisch unmöglich macht, daß Datenmißbrauch durch eine totale Öffentlichkeit aller Daten verhindert werden könnte“,[1187] sind in diesem Zusammenhang zu sehen, denn sie setzen voraus, dass tatsächlich, d. h. eben auch technisch, alle Daten öffentlich gemacht werden könnten, und das zeigt zugleich die strukturellen Grenzen der Open-Data-Ideologie auf. Auch die derzeit geführte Diskussion um „Metadaten“ wird dort bereits vorweg genommen, wo etwa Steinmüller in seinem Vortrag darauf hinweist, dass diese Metadaten, die er als „Prozeßdaten“ bezeichnet und die „durch die Interaktion von Menschen mit dem System entstehen“, und „ihr scheinbar zwangsläufiges Entstehen und weiteres Schicksal von dem Abgebildeten häufig nicht bemerkt sowie kaum je mitgestaltet und mitverantwortet werden kann.“[1188] Und nicht zuletzt lehnt Steinmüller auch die Behauptung ab, dezentrale Strukturen seien immer datenschutzfreundlicher als zentrale – stattdessen hänge dies von den jeweiligen Umweltbedingungen ab, denn dezentrale Systeme könnten „so vertrackt organisiert sein, daß sie kein Mensch mehr politisch angreifen kann.“[1189]

In der öffentlichen und publizistisch geführten Diskussion lag der Schwerpunkt am Ende des Jahrzehnts jedoch weniger auf der neuen Technik und ihren Möglichkeiten, sondern klar auf dem sich vertiefenden Überwachungsstaat, dessen Gebaren gerade 1978 in einer langen Reihe von Skandalen ans Licht der Öffentlichkeit gezerrt worden war.[1190] Während Horst Herold, damaliger Präsident des Bundeskriminalamtes, jedenfalls in seinen Veröffentlichungen einem Primat

[1185] Fred Grätz in der Diskussion über die Gefahren, die durch „das Ablesen der Gas- und Stromzähler über den Rückkanal“ enstehen könnten, siehe Dette et al. (1979, S. 71).

[1186] Siehe zu den datenschutzrechtlichen wie -technischen Fragen und zu den Möglichkeiten einer datenschutzgerechten Technikgestaltung von Fernwirkdiensten Schrempf (1990).

[1187] Dette et al. (1979, S. 79).

[1188] Siehe Steinmüller (1979d, S. 84 f.).

[1189] Die Äußerung fällt in der Diskussion zu seinem Beitrag, siehe Dette et al. (1979, S. 99). Die dort angesprochene Angreifbarkeit entspricht dabei offensichtlich dem später von Rost und Pfitzmann in die Diskussion eingebrachten Konzept der Intervenierbarkeit, siehe Rost und Pfitzmann (2009), siehe dazu auch die dort schon aufkommende Diskussion zu den Möglichkeiten direkter, d. h. technik-gestützter und nicht von der Organisation beeinflussbarer, Intervention durch die Betroffenen, die von Ingrid Lottenburger angestoßen wurde, und Bulls Ergänzung um die Forderung nach eingebauter Kontingenz, Dette et al. (1979, S. 127 f.).

[1190] Siehe die Auswahl bei Bölsche (1979, S. 15) sowie die umfassende Darstellung bei Foschepoth (2013, S. 232 ff.).

von Effizienz gegenüber den Grundrechten eine Absage erteilt,[1191] wirft Hans Magnus Enzensberger ihm – und „den Seinen“ – genau das vor.[1192] Mehr noch: Es gehe ihnen mehr um die Zukunft als die Vergangenheit, nicht nur um Repression, sondern um „die präventive Planung einer kybernetisch gesteuerten, störungsfreien Gesellschaft.“ Die Polizei solle zu einem „Early Warning System“ entwickelt werden, das „Fehlentwicklungen und Risiken entdeckt und politische Strategien entwirft“, „Gefährdungen der »Sicherheit« aufspürt und eliminiert, bevor sie massenhaft auftreten können“[1193] – heute diskutiert als „predictive policing“ und dabei oft genug als „neue Entwicklung“ verkauft.[1194] Die Realität überwachungsstaatlicher Maßnahmen, die Einführung und Vergrößerung staatlicher Überwachungssysteme, die nachträgliche Legalisierung bestehender sowie die Schaffung gesetzlicher Grundlagen für neue Überwachungspraktiken[1195] – sie alle sprechen weniger von der staatlichen Selbstbeschränkung, deren Existenz Herold behauptet, als vom Weg „vom Verfassungs- zum Sicherheitsstaat“.[1196] Und alle Versuche, diesen Vorwurf als unbegründet zu enttarnen, scheinen dann scheitern zu müssen, wie das Beispiel von Hans Peter Bull, dem ersten Bundesdatenschutzbeauftragten, zeigt: Um nachzuweisen, „daß [...] »keineswegs« ein großer Teil der Bevölkerung von den Sicherheitsorganen »in irgendeiner Weise überwacht wird«“, versuchte er, die Dienste zur Offenlegung der Zahl der „Bürger-Dossiers“ zu bewegen – erfolglos.[1197]

Zu den wenigen, die weiterhin auf einer grundlegenden Analyse des Datenschutzproblems bestanden, gehörte Steinmüller, der dabei seine vorher getätigten Ausführungen[1198] erweiterte, vertiefte und in eine veritable Theorie der Industrialisierung der Informationsverarbeitung münden ließ,[1199] Datenschutz – bei Steinmüller mal mehr, mal weniger deutlich in „Datenschutz im engeren Sinne“ und „Datenschutz im weiteren Sinne“ unterteilt – diene dabei dazu, „angesichts der rapide fortschreitenden Datenerfassung aller Lebensbereiche [...] noch diejenigen politischen, sozialen und individuellen Handlungsspielräume zu erhalten (oder gar zu verbessern), die für eine funktionierende Demokratie mit mündigen Bürgern (über)lebensnotwendig

[1191] So das Fazit seiner Ausführungen, wonach „Datenschutz im Rahmen polizeilicher Informationssysteme den bewußten und gezielten Verzicht auf die Vollständigkeit von Informationen, den Verzicht auf die unverhältnismäßige Steigerung von Effizienz“ bedeute und Effizienz „gegenüber Menschen nicht der alleinige Maßstab“ sein dürfe, siehe Herold (1980, S. 84).

[1192] Siehe etwa Enzensberger (1979b), und dessen Kurzfassung im Spiegel, Enzensberger (1979a). Der Spiegel hatte kurz zuvor eine mehrteilige Serie zu staatlicher Überwachung publiziert, die der Autor anschließend zusammen mit ausgewählten Dokumenten und Stellungnahmen als Buch veröffentlichte, siehe Bölsche (1979).

[1193] Enzensberger (1979b, S. 11). „[D]ie Polizisten“ würden „an einem großen Entwurf basteln“, siehe S. 14: „Sie wollen uns ein Neues Atlantis der allgemeinen Inneren Sicherheit bescheren, einen sozialdemokratischen Sonnenstaat, eine Insel Felsenburg für Sozialautomaten, gelenkt und gesteuert von den allwissenden und aufgeklärten Hohepriestern des Orakels von Wiesbaden.“

[1194] Die andere, damals stark diskutierte „Methode“ neben dem „predictive policing“ war die Rasterfahndung, siehe Herold (1980, S. 82 f.), die in der amerikanischen Diskussion meistens als „computer matching“ bezeichnet wurde, siehe etwa Shattuck (1984). Beide können aber auch zusammen auftreten, denn Rasterfahndung und „computer matching“ sind im wesentlichen Operationen auf Datenebene, während „predictive policing“ eine Klasse von Verfahren auf Organisationsebene – und mithin auf Informationsebene – meint.

[1195] Siehe die Übersicht bei Steinmüller (1979a).

[1196] Steinmüller (1979a, S. 169). Herold zog gegen Steinmüller wegen dieses Artikels vor Gericht und unterlag, siehe Bölsche (1979, S. 18).

[1197] Siehe Bölsche (1979, S. 14).

[1198] Vor allem Steinmüller (1975a) und Steinmüller (1979c).

[1199] Der Weg lässt sich deutlich nachzeichnen von Steinmüller (1979c) über Steinmüller (1979b), Steinmüller (1980c) und Steinmüller (1980b) bis zu Steinmüller (1981). Siehe dazu auch Pohle (2016c). Zu einer anderen historisch-gesellschaftlichen Einordnung – nämlich als „Control Revolution“, die bereits nach 1830 begonnen habe – siehe Beniger (1986), siehe zur wissenschaftshistorischen Einordnung der modernen Informationsverarbeitung und des Datenschutzes auch Podlech (1976a, S. 23 f.).

sind.“[1200] Einen eingeschränkteren Blick auf das Problem hat Herbert Meister, der als „Schutzgut des Datenrechts“[1201] das „Recht am eigenen Datum“ als „Selbstdarstellung des Menschen“ auf der Basis einer „Rollenanalyse“, die sich einer Bindung an einen bestimmten Diskussions- und Theoriestrang in der sich auf das Konzept der „Rolle“ beziehenden Soziologie verweigert, identifizieren will.[1202] Zwar solle diese Kontrolle über die Selbstdarstellung „Autonomie für individuelles Handeln“ schaffen,[1203] es gibt jedoch keine – vor dem Hintergrund der Behauptung einer Bezugnahme auf die „Datenverarbeitung im weitesten Sinn“ eigentlich notwendige – Diskussion über die Suffizienz dieser Kontrolle für die Autonomie.

Gleichzeitig zeigen die Veröffentlichungen Ende der 70er und Anfang der 80er Jahre aber auch, dass selbst nach dem Inkrafttreten des Bundesdatenschutzgesetzes die erreichten Erkenntnisse und Positionen keineswegs als gesichert gelten können – alles bleibt fundamental umstritten. So fällt etwa Podlech in seiner Darstellung von Art. 2 Abs. 1 GG hinter den Stand der Diskussion zurück, indem er seinen Kern als Schutz von „Privatheit“ fasst, diese „Privatheit“ erst von der „freien Entfaltung der Persönlichkeit“ abgrenzt,[1204] anschließend allerdings die „freie Entfaltung der Persönlichkeit“ neben der „informationellen Selbstbestimmung“ und der „Achtung des privaten Bereichs“ als dritten Teil der „sachlichen Dimension“ dieser „Privatheit“ zu identifizieren meint.[1205] Das ganze krönt er dann, indem er die „Privatheit“ in der „Privatsphäre“ verortet und diese von der „Öffentlichkeit“ – dem „Politischen“ – abgrenzt,[1206] in der Diskussion zur „sachlichen Dimension des Rechts der Privatheit“ allerdings – insbesondere für die „informationelle Selbstbestimmung“ – ganz selbstverständlich wieder davon ausgeht, dass die Handlungen in der „Öffentlichkeit“ damit geschützt würden, sowohl vor dem Staat wie vor Privaten,[1207] um zuletzt aber wieder den „Heraustritt aus der Privatheit“ als eigenständiges Problem aufzuwerfen.[1208] Auch Bull sieht auf der grundsätzlichen Ebene eine solche Trennung zwischen dem allgemeinen Persönlichkeitsrecht, das einen „starken Bezug zum Recht der persönlichen Ehre“ besitze, und der „Privatsphäre“, die er als Übersetzung von „privacy“ betrachtet, auf „Selbstbestimmung und Entfaltungsfreiheit“ abbildet und sie zugleich als sowohl räumlich wie nicht-räumlich bezogen bezeichnet.[1209] Auf diese „Privatsphäre“ beziehe sich das Datenschutzrecht, mit dem erstmalig – jedenfalls in dieser Breite – „die *Verteilung von Informationen* zum Gegenstand von Rechtsnormen“ werde, ähnlich der Regelung der „Güter- oder Macht-(Kompetenz-)Verteilung“, mit der „zumindest teilweise beabsichtigt[en]“ Folge einer „Informationsrationierung“ als einem „Mittel der Machteinschränkung“.[1210] Mit dieser Vorverlagerung zeige sich das Datenschutzrecht zugleich als „Recht der *Gefahrenabwehr*“ mit einer Ähnlichkeit zur Gefährdungshaftung – eine

[1200] Steinmüller (1979b). Zu dieser Gefahr einer der Erhaltung und Ausdehnung der Handlungsspielräume entgegengesetzten Vorstrukturierung menschlichen Handelns durch übermächtige Organisationen, deren Machterhalt und Machtposition durch den Technikeinsatz sichergestellt und erweitert zu werden droht, siehe auch Lenk (1982).

[1201] So der Titel seines Artikels, Meister (1983). Mit „Datenrecht“ will er „ein Spektrum [adressieren], das alle Fragen umfaßt, die mit der Datenverarbeitung im weitesten Sinn Zusammenhängen“ (S. 163).

[1202] Siehe Meister (1983, S. 167, 168, 170 ff.).

[1203] Siehe Meister (1983, S. 169).

[1204] Siehe Podlech (1979, S. 50).

[1205] Siehe Podlech (1979, S. 52).

[1206] Siehe Podlech (1979, S. 52 f.).

[1207] Siehe Podlech (1979, S. 55 ff.).

[1208] Siehe Podlech (1979, S. 62 ff.).

[1209] Siehe Bull (1979, S. 1179). Etwas später wird sich Bull allerdings – jedenfalls vorläufig – davon verabschieden, die „Privatsphäre“ für den Grund für Datenschutz zu halten, und stattdessen auf die „Ordnung des Informationswesens“ rekurrieren, siehe Bull (1981a, S. 874).

[1210] Siehe Bull (1979, S. 1179).

Tatsache, die Bull jedoch kritisiert, da es auch reichen könne, „mit den Gefahren zu leben, ihre *Realisierung* abzuwehren und dennoch eintretende Schäden auszugleichen". Einen solchen Ansatz sieht Bull nur aufgrund der nur geringen „praktischen Möglichkeiten, einen Fehlgebrauch [sic!] von Informationen rechtzeitig abzuwehren"[1211] – hier fehlt ihm offensichtlich die Sachkenntnis, die vorhergegangene Diskussion zum Problem von Modellannahmen zu reflektieren.[1212] Auch die von ihm identifizierten vier Gruppen Bedrohungen, von denen aus sich die „schutzwürdigen Belange der Betroffenen" erst richtig erfassen ließen, – „*Neugierde*", „daß Daten »*kommerzialisiert*« werden", „*Gefahren für die persönliche Entfaltung des einzelnen*" und „daß *illegitime Herrschaft* über Menschen ausgeübt wird"[1213] – lassen Fragen offen, nicht nur weil Bull keinerlei Erklärung für seine Klassifizierung gibt. Die ersten beiden Klassen scheinen sich auf Befindlichkeiten zu beziehen, denn er beginnt die Beschreibung der ersten Gruppe mit einem Verweis darauf, dass es „[v]ielen [...] unangenehm" sei, und bezeichnet in seinen Ausführungen zur zweiten Gruppe die Kommerzialisierung als „Ärgernis". Auch ist die Trennung zwischen der dritten und der vierten Gruppe unklar: Die dritte verweise auf „Bedrohungen durch berufliche, wirtschaftliche oder sonstige soziale Nachteile von Gewicht", während die vierte „die laufende Überwachung und Kontrolle des einzelnen" beschreibe – als seien diese keine „sozialen Nachteile von Gewicht". Noch extremer liegt der Fall bei Michael Kloepfer, der an einer dichotomen Trennung von Staat und Gesellschaft festhält, Datenschutz im wesentlichen nur als Geheimnisschutz – „Personengeheimnis" nennt er diesen Kern seines Konzepts von „Privatsphäre" – sehen und dafür selbst auf die Sphärentheorie nicht gänzlich verzichten will, obwohl ihm deren Untauglichkeit bekannt ist.[1214] Um zu diesem Ergebnis zu gelangen, operiert er vorwiegend über falsche Zuschreibungen, Strohmann-Argumente und der Auslassung von Gegenargumenten.[1215] Das gilt ebenso für Rudolf Schomerus, der etwa zum Verbot mit Erlaubnisvorbehalt meint, es behafte Datenverarbeiter „mit dem Image des Gefährlichen, Bedrohlichen", und unterstelle ihnen, „prinzipiell Unrechtes zu tun", und stattdessen vom „Sensibilitätsgrad der Daten" fabuliert.[1216] Datenverarbeitung sei gerade nicht „generell als gefährlich und damit regelungsbedürftig" zu betrachten, weil es „eine Ausdrucksform der Kommunikation" und „Kommunikation [...] grundsätzlich positiv zu bewerten" sei: „Kommunikation muß prinzipiell frei sein."[1217] Etwas reflektierter, wenn auch immer noch mit dem Strohmann der „Privat(daten)sphäre"[1218] hantierend, sind immerhin die soziologischen Ausführungen von Volker Ronge – von einzelnen absurden Behauptungen abgesehen, wie der, dass es im Bereich der öffentlichen Verwaltung nur darum gehen könne zu sichern, dass gespeicherte Daten „nicht »vagabundieren« und von Unbefugten in eigenem Inter-

[1211] Siehe Bull (1979, S. 1180).
[1212] Siehe dazu Harbordt (1975, S. 72 ff.).
[1213] Siehe dazu und zum folgenden Bull (1979, S. 1180 f.).
[1214] Siehe Kloepfer (1980).
[1215] Siehe dazu etwa seine Ausführungen zur „Dämonisierung des Computers" (S. 10), zur „Verstaatlichung der Gesellschaft" (S. 11), zur „generellen Staatsverhinderung" durch den datenschutzrechtlichen Gesetzesvorbehalt (S. 23) – wahrscheinlich ähnlich der „generellen Staatsverhinderung" durch den allgemeinen Gesetzesvorbehalt –, zur Frage eines „schrankenlos gewährten Datenschutzgrundrecht[s]" (S. 28) oder zur durch nichts begründeten Behauptung, „[m]an kann nicht ein gläsernes System schaffen wollen und dann zugleich den gläsernen Menschen beklagen" (S. 53) – eine Behauptung, mit der Kloepfer die gesamte geltende Verfassungsordnung mit einem Federstrich auf den Kopf stellt.
[1216] Siehe Schomerus (1981, S. 292).
[1217] Schomerus (1981, S. 294). Siehe dazu aber auch die Verordnung (EG) Nr. 1924/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über nährwert- und gesundheitsbezogene Angaben über Lebensmittel, ABl. L 404 vom 30.12.2006, S. 9, mit der für gesundheitsbezogene Werbeaussagen, die wohl unzweifelhaft „Kommunikation" sind, ein Verbotsprinzip mit Erlaubnisvorbehalt eingeführt wurde.
[1218] Ronge (1981, S. 110).

esse verwendet werden können."[1219] Seine Kritik an dem Gesellschaftsbild, das er „hinter dem restriktiven rechtlichen Schutz personenbezogener Daten" sieht, – anzunehmen, das Individuums sei „die entscheidende »soziale« Einheit", dass „die Individuen in einem Verhältnis (der Konkurrenz) zueinander stehen, das sie nötigt, sich gegeneinander zu schützen" und dass „die Individuen als Gesamtheit in einem Verhältnis zu »ihren« sozialen Institutionen, insbesondere dem Staat, das von Mißtrauen geprägt ist", d. h ein „frühbürgerliche[s] bzw. frühkapitalistische[s] Gesellschaftsmodell"[1220] – trifft auf einen wesentlichen Teil der Privatheits- und Datenschutzdebatte zu, allerdings nicht auf alle: Es geht nicht bei allen diesen Ansätzen um „den Schutz von Daten", sondern um den Schutz vor Datenverarbeitern; nicht bei allen geht es um den Schutz der Individuen „gegeneinander", sondern um den Schutz vor Organisationen; und das Misstrauen gegenüber sozialen Institutionen wie dem Staat ist auch nicht allein „frühbürgerlich[] bzw. frühkapitalistisch[]", sondern ganz allgemein „bürgerlich" im Sinne des Schutzes vor sozial, ökonomisch und politisch mächtigen Akteuren.[1221] Damit werden auch die beiden Alternativen, die Ronge dann anspricht, als fehlerhaft enttarnt: die „informierte" Gesellschaft mit der „Flucht in die Öffentlichkeit" und dem „Leben im Glashaus"[1222] und die „nachmoderne", postindustrielle Gesellschaft, die dann wieder eine segmentäre sein soll.[1223] Der erste Alternativentwurf ignoriert das von Organisationen ausgehende Machtproblem, der zweite ist eine Flucht in romantische Vorstellungen von einer nicht-entfremdeten Welt, zugleich jedoch ein gesellschaftlicher Rückschritt.

Ronge ist aber nicht der einzige, der die wissenschaftliche Forschung als im Konflikt mit dem Datenschutz stehend sieht, auch wenn sein Ziel wohl in erster Linie darin besteht, den Datenschutz zurückzustutzen.[1224] In einer Kolloquienreihe wurden diese Fragen ausgiebig diskutiert, im Ergebnis wird allerdings weniger eine Überreaktion des Datenschutzes kritisiert als vielmehr das Scheitern des Datenschutzrechts, die „die Datenflüsse innerhalb von Behörden zu kontrollieren und transparent zu machen", und zugleich die „weitgehende Abschottung des amtlichen Datensystems gegenüber Wissenschaft und Öffentlichkeit" mit der Folge der Unmöglichkeit, „die mit Daten vorgenommenen Begründungen von Politik kritisch zu überprüfen."[1225] Einen Schwerpunkt in den Vorträgen und Diskussionen nimmt der Topos der Anonymität ein, einerseits grundsätzliche Fragen danach, was Anonymität ist und wie anonym anonyme oder anonymisierte Informationen tatsächlich sind, andererseits technische und organisatorische Verfahren zur vollständigen oder faktischen Anonymisierung.[1226] Daneben bringt Müller einen Vorschlag

[1219] Ronge (1981, S. 113), indem er offensichtlich einzig Personen als mögliche Angreiferinnen sieht, nicht jedoch Organisationen, und das Problem ausschließlich in der Weitergabe verortet, nicht in Erhebung oder Nutzung. Beide Lücken bleiben dabei vollständig unbegründet. Wahrscheinlich folgt dies aus der Überbetonung von „Missbrauch" als Gefährdungstatbestand, siehe S. 115.

[1220] Siehe Ronge (1981, S. 120).

[1221] Siehe dazu Pohle und Knaut (2014, S. 161 f., Rn. 119).

[1222] Siehe Ronge (1981, S. 121) mit Verweis auf Haefner (1980).

[1223] Siehe Ronge (1981, S. 123 ff.).

[1224] Siehe Ronge (1981, S. 115 ff.).

[1225] Siehe Kaase et al. (1980). Die einzige Ausnahme davon stellt Scheuch dar, der es als Mitherausgeber offensichtlich vermieden hat, die anderen Beiträge zu lesen, und jedenfalls auch sonst nicht gerade zeigt, dass er sich in der Materie auskennt, siehe Scheuch (1980). So glaubt er, aus der Problematisierung der Verwendung von personenbezogenen Informationen als dem zentralen Problem begründungslos schließen zu können, dass damit alle anderen Phasen unproblematisch sind (S. 262 ff.), obwohl sein eigener Mitarbeiter Paul Müller ausführlich Gegenteiliges nachwies, siehe etwa Müller (1975c).

[1226] Siehe etwa zur Frage der Operationalisierung von Personenbezug von Informationen Brennecke (1980), zum Zusatzwissen Burkert (1980), zu technischen Fragen der Anonymisierung Schlörer (1980) und Cox (1980) sowie zu verfahrensbasierten Anonymisierungsansätzen Steinmüller (1980a). Dabei wird umfangreich auf eine

wieder auf, den schon Miller Anfang der 1970er diskutierte: die Einrichtung von „Datentreuhändern“.[1227] Diese Treuhänder würden dabei nicht nur im Rahmen der Anonymisierung von Forschungsdaten eine wichtige Rolle spielen können, sie wäre zugleich eine praktische Umsetzung einer datenschutzfreundlichen Organisationsgestaltung durch informationelle Gewaltenteilung.

Die internationale Debatte über den Schutz und die Regulierung von *privacy* und Datenschutz kulminierte Ende der 70er und Anfang der 80er in zwei richtungsweisenden Entscheidungen. Nachdem die OECD schon seit Ende der 60er Jahre erste Diskussionen zum Umgang mit dem *privacy*-Problem führte,[1228] beschloss sie im September 1980 die „Guidelines on the Protection of Privacy and Transborder Flow of Personal Data“.[1229] Eines der wesentlichen Ziele der OECD bestand darin zu verhindern, dass die nationalstaatlichen Regulierungen von *privacy* und Datenschutz zu einer Beschränkung des „freien Informationsflusses“ führten, der dazu als Prinzip konstruiert wurde, das als gleichberechtigt neben die *privacy*- und Datenschutzinteressen von Betroffenen gestellt mit diesen abgewogen werden müsse. Kurz darauf hat der Europarat mit der Konvention 108 zum „Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ den ersten völkerrechtlich verbindlichen Vertrag zum Datenschutz abgeschlossen.[1230] Auch der Konvention wird – schon in der Präambel – die Auffassung zugrunde gelegt, dass der freie Informationsfluss an sich schützenswert sein soll und daher „die grundlegenden Werte der Achtung des Persönlichkeitsbereichs und des freien Informationsaustausches zwischen den Völkern in Einklang zu bringen“ seien. Dieses Prinzip ist dabei – insbesondere in der vorliegenden Formulierung – jedoch offensichtlich nur vorgeschoben, denn in der Konvention geht es an keiner Stelle um den „freien Informationsaustausch zwischen den Völkern“, sondern – trotz der Einbeziehung natürlicher Personen in die Liste der „Verantwortlichen“ nach Artikel 2 Nr. d – sehr deutlich um Organisationen, wie die Anforderungen in Artikel 5 der Konvention zeigen.[1231]

Wenn – wie von den meisten Beobachterinnen, insbesondere den Juristinnen und insbesondere in der Bundesrepublik vertreten – die Entscheidung des Bundesverfassungsgerichts im Verfahren um die Verfassungsmäßigkeit des Volkszählungsgesetzes als historische Zäsur betrachtet wird, dann erlangen leicht die Arbeiten, die vor der Entscheidung abgeschlossen und zumindest in großer zeitlicher Nähe dazu veröffentlicht wurden, den Nimbus des Veralteten, die – quasi überrollt von der Geschichte – ein letzter Abklatsch der überwundenen Vorstellungen und Paradigmen der alten Zeit sind. Vielleicht lässt sich jedenfalls so erklären, warum Podlechs Ar-

schon länger stattfindende Auseinandersetzung zu Anonymität und Anonymisierung in der wissenschaftlichen – sowohl in der statistischen wie in der informatischen – Literatur verwiesen, siehe etwa Dalenius (1977), Cox (1978) und Rivest et al. (1978), letztere mit der Präsentation ihrer Idee von „privacy homomorphisms“, Verschlüsselungen, die es erlauben, Operationen auf verschlüsselten Daten auszuführen, ohne die Daten vorher entschlüsseln zu müssen. Siehe auch die Übersicht zu den bereits diskutierten und entwickelten Schutztechniken bei Schlörer (1980, S. 133 f.). Die meisten grundlegenden Ansätze für eine Anonymisierung von Daten, die heute oft der Forschung ab Ende der 1990er Jahre – etwa mit Samarati und Sweeney (1998) – zugerechnet werden, stammen tatsächlich schon aus den 1970ern, wie sich hier zeigt.

[1227] Siehe Müller (1980), und zur Diskussion Anfang der 1970er Jahre siehe Miller (1971, S. 216 ff.).

[1228] Siehe das erste Ergebnis dieser Debatten, Niblett (1971).

[1229] Organization for Economic Cooperation and Development, ICCP Subcommittee, Guidelines on the Protection of Privacy and Transborder Flow of Personal Data (C(80)58/FINAL) vom 23. September 1980. Siehe zur Diskussion der Entwicklung und Weiterentwicklung dieser Prinzipien die Darstellungen des damaligen Vorsitzenden der Kommission, Michael Kirby, Kirby (1999), Kirby (2003) und Kirby (2011), zur aktuellen Neufassung der Prinzipien Cate et al. (2013) sowie die Selbstdarstellung aus der Sicht der OECD OECD (2011).

[1230] Europarat, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) vom 28. Januar 1981.

[1231] So im Ergebnis auch Bergmann (1987, S. 209 ff.), der zugleich auf ein Gegenbeispiel hinweist: die Empfehlungen des Europäischen Parlaments vom 8. Mai 1979.

beit „Individualdatenschutz – Systemdatenschutz“[1232] so wenig Aufmerksamkeit erregte und so wenig rezipiert wurde, obwohl Podlech hier – jedenfalls im Rückblick – zum ersten Mal Anforderungen des Datenschutzes in Form von Schutzzielen formulierte – eine Form der abstrakten Operationalisierung zur Herstellung interdisziplinärer Anschlussfähigkeit bei gleichzeitiger Aufrechterhaltung der jeweiligen Eigenlogiken der Disziplinen und der Vermittlung zwischen Sein und Sollen, wie sie für den Datenschutz erst wieder von Martin Rost und Andreas Pfitzmann fast 30 Jahre später vorgelegt wurde.[1233] Für Podlech dient „Individualdatenschutz“ „der Wahrung von Interessen der Betroffenen“, während „Systemdatenschutz“ – der „strukturelle[]“ oder „systemanalytische[] Aspekt“ von Datenschutz – von vornherein die Gesellschaft insgesamt in den Blick nimmt und „Vorgänge der Informationserhebung und Informationsverarbeitung unabhängig davon, ob im Einzelfall Interessen der Betroffen berührt sind oder nicht, rechtlich so ordne[t], daß die Gesamtheit der rechtlich geregelten Informationsvorgänge keine sozialschädlichen Folgen herbeiführen.“[1234] Die von Podlech formulierten Prinzipien des Systemdatenschutzes umfassen dabei die „Transparenz des Informationsverhaltens“, die „Beschreibbarkeit der Erforderlichkeitsrelation“, das „Verbot hyperkomplexer Verwaltungstätigkeit“, das „Gebot der Validität und Verbot der Kontextveränderung“ sowie das Gebot der „Sicherung der Rechtspositionen von Betroffenen“.[1235] Diesen Topos greift Podlech auch in seinem informationsrechtlichen Gutachten zum Datenschutz im Vertrauensärztlichen Dienst auf, wo er Datenschutz als Antwort auf das Problem bezeichnet, „daß die Machtstrukturen moderner Gesellschaften und die gesellschaftlich verwirklichten technischen Möglichkeiten ein Informationsverhalten staatlicher und gesellschaftlicher Systeme (z. B. von Behörden oder Unternehmen) provozieren, das für die einzelnen Glieder der Gesellschaft nicht mehr akzeptabel zu sein braucht und das damit die Konsensgrundlage der Rechtsordnung zu erschüttern in der Lage ist“,[1236] ihn jedoch zugleich wiederum nur auf jenen Teil des vorher angesprochenen Problems beschränken, der „es mit personenbezogenen Informationen und also mit einzelnen Betroffenen zu tun hat“.[1237] Diese Beschränkung bleibt allerdings erstens unbegründet, und zweitens erklärt Podlech nicht, warum das Informationsverhalten nur dann mit einzelnen Betroffenen zu tun hat, wenn es auf personenbezogenen Informationen basiert. Darüber hinaus präsentiert er geänderte und anders eingeordnete Prinzipien von Individual- und Systemdatenschutz:[1238] Zum Individualdatenschutz zählt er hier das „Prinzip der Bindung durch rechtliche Kompetenzzuweisung“, das „Prinzip der adäquaten Kompetenzzuweisung“, das „Prinzip der aufgabenadäquaten Form einer Informationsspeicherung“ sowie das vorher dem Systemdatenschutz zugeordnete „Prinzip der Wahrung individueller Rechtspositionen“, während er die „Transparenz des Informationsverhaltens“, die „Beschreibbarkeit der Erforderlichkeitsrelation“, die „Modelladäquanz“, das „Gebot der hinreichenden Validität“ sowie das „Verbot der Kontextänderung“.[1239] Anschließend zeigt Podlech

[1232] Podlech (1982).

[1233] Siehe dazu Rost und Pfitzmann (2009), Rost und Storf (2013) und Hansen et al. (2015). Dass Podlechs Datenschutzziele – von ihm als „Datenschutzprinzipien“ bezeichnet – dies auch leisten sollen, ergibt sich aus Podlechs Verständnis von „umfassende[r] informationsrechtliche[r] Bewertung“, der die Datenschutzprinzipien dienen sollen, siehe Podlech (1983, S. 206).

[1234] Siehe Podlech (1982, S. 451 ff.).

[1235] Siehe Podlech (1982, S. 454 ff.).

[1236] Siehe Podlech (1983, S. 201). Auch diese Arbeit ist in Wissenschaft und Praxis fast nicht rezipiert worden.

[1237] Siehe Podlech (1983, S. 202).

[1238] Er beschränkt sich dabei auf eine Auswahl der Prinzipien, nämlich diejenigen, die er der Begutachtung zugrunde gelegt hat, siehe Podlech (1983, S. 207).

[1239] Siehe Podlech (1983, S. 207 ff.).

einen ersten Versuch einer ordentlichen datenschutzrechtlichen Analyse der Interessen aller mit dem Informationssystem verbundenen Akteurinnen.[1240]

Das Gegenbeispiel zu Podlechs Arbeiten ist die Dissertation von Hans-Georg Woertge, der im Vorwort seiner vor dem Urteil abgeschlossen und nach dem Urteil veröffentlichten Arbeit darauf verweisen kann, dass das von ihm besprochene Recht auf informationelle Selbstbestimmung vom Bundesverfassungsgericht in den Rang eines Grundrechts gehoben wurde, wenn auch nicht nur gestützt auf Art. 2 Abs. 1 wie in der Darstellung bei Woertge, sondern auf das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[1241] In seiner Arbeit versucht Woertge, das Datenschutzrecht in seiner Systematik darzustellen. Er ist dabei einer der ganz wenigen, die überhaupt versuchen zu explizieren – und das nicht nur als gegeben hinnehmen –, warum das Datenschutzrecht um den Begriff „Datum“ – im Sinne eines Informationsbegriffs – und die Informationskontrolle herum gestaltet ist: „Dieses Erfordernis beruht auf der Feststellung, daß menschliches Handeln interessen-, zweck- und zielorientiert ist und hierbei Informationen die Grundlage der Entscheidung für ein bestimmtes Verhalten bilden.“[1242] Der Datenschutz, so Woertge, betreffe „die Informationen, die geeignet sind, das in der Rechtsgemeinschaft relevante menschliche Handeln zu beeinflussen“,[1243] aber gleichwohl nicht alle – Datenschutz sei kein „Mittel zur Erreichung einer angemessenen Informationsverteilung“, denn das sei mit dem Prinzip der Privatautonomie nicht vereinbar[1244] –, sondern diene dazu, „bestimmte Gefahren für rechtlich geschützte Positionen abzuwehren“ – sowohl die Grundrechte wie alle subjektiven privaten Rechte.[1245] Die Darstellung der Gefahren ist vor dem Hintergrund der zu diesem Zeitpunkt bereits seit Jahrzehnten geführten Diskussion reichlich oberflächlich und ein Sammelsurium aus Technikeigenschaften – Maschinen könnten „ein Vielfaches an Daten [...] speichern“ –, Technikfolgenzuschreibungen – „der einzelne sich resignierend auf die Allmacht des Computers verläßt“ –, interpersonalen Rollenbeziehungen – „gegenüber Nachbarn“ –, der Strukturierungsmacht von Organisationen und der Degradierung des Menschen zum Objekt oder zur Nummer.[1246] Woertge nimmt seine Systematisierung des Datenschutzrechts nach Normzwecken, d. h. den Schutzgütern der oben angesprochenen Normen, vor,[1247] die er in vier große thematische Gruppen – Schutz der Menschenwürde, Schutz der Privatsphäre, Schutz der Betätigungsfreiheit und Sicherung des Informationsgleichgewichts – und eine Sammelgruppe für alles, was er sonst nicht unterbringen konnte, einteilt.[1248] Abgesehen vom Verbot einer Registrierung des Menschen „in seiner gesamten Persönlichkeit“ und der Verhinderung von „Verängstigung“ mit der Folge von *chilling effects* für die Grundrechtsausübung bleiben die Ausführungen zur Menschenwürde für Woertges wei-

[1240] Siehe Podlech (1983, S. 213 ff.).
[1241] Siehe Woertge (1984, S. VII f., 29 ff., 70 f.).
[1242] Woertge (1984, S. 21).
[1243] Woertge (1984, S. 21 f.).
[1244] Siehe Woertge (1984, S. 24).
[1245] Siehe Woertge (1984, S. 25, 29 ff.), der daneben den von Steinmüller und seinen Mitautorinnen so genannten Institutionaldatenschutz stellt (S. 26).
[1246] Siehe Woertge (1984, S. 26 ff.). Siehe aber auch die Darstellung auf S. 35 zu den Rechtssubjekten, die darauf hindeutet, dass Woertge Individuen nicht primär als Datenverarbeiter problematisiert.
[1247] Siehe Woertge (1984, S. 39).
[1248] Siehe Woertge (1984, S. 54 ff.).

tere Ausführungen folgenlos.[1249] Die Ausführungen zur „Privatsphäre“ sind nicht hilfreicher.[1250] Woertge behauptet, es bestehe „Einigkeit darüber, daß zumindest ein Ziel die Verteidigung der Privatsphäre ist“, muss aber zugleich zugeben, dass unklar sei, was deren Schutzbereich sei, um dann Privatsphäre als Verfügungsrecht über „seine eigenen Daten“ und als Schutz „gegenüber der ihn betreffenden Datenverarbeitung anderer“ zu beschreiben, Privatsphäre mit einem „Recht auf Freiheit“ gleichzusetzen und schlussendlich als Schutzbereich „die Verarbeitung personenbezogener Daten“ zu „finden“.[1251] Anschließend versucht Woertge, „objektive Kriterien zu finden, die bei einer bestimmten Form der Datenverarbeitung für oder gegen eine Schutzbedürftigkeit des Betroffenen sprechen können“,[1252] einmal die eigenen Vor- und Nachteile für die Betroffene,[1253] zum anderen den „Gefährdungsgrad“ – die Art der datenverarbeitenden Stelle, die Art der Datenverarbeitung, die Art der Daten und die Intensität des Eingriffs.[1254] Der Schutz der Betätigungsfreiheit wird von Woertge ausschließlich unter dem Gesichtspunkt der Betätigungsfreiheit der Datenverarbeiter – und zwar sowohl der privaten wie der öffentlichen – behandelt.[1255] Insgesamt bleibt die Arbeit weit hinter ihren Möglichkeiten zurück, auch weil weder die Systematisierung der Prinzipien noch die anschließende Untersuchung ihrer Realisierung im Datenschutzrecht wesentliche neue Erkenntnisse zeitigt.

Anfang der 80er Jahre begann auch die erste Reihe von Versuchen, das Bundesdatenschutzgesetz zu überarbeiten und zu ergänzen[1256] oder die Grenzen des bestehenden Datenschutzrechts

[1249] Siehe vor allem Woertge (1984, S. 57 ff.). Das ist in beiden Fällen nicht überraschend: „In seiner gesamten Persönlichkeit“ wird nie jemand „registriert“, denn selbst eine „vollständige“ Registrierung braucht immer nur die Informationen aus dem *für den Datenverarbeiter relevanten* Teil der Persönlichkeit, *aber nicht alle*. Und die Diskussion zu den *chilling effects* gehört grundsätzlich nicht zu Art. 1 GG, sondern zu den Grundrechten, vor deren Ausübung abgeschreckt wird.

[1250] Siehe dazu und zum folgenden Woertge (1984, S. 60 ff.). Siehe dazu auch seine – eigentlich von seiner „Privatsphäre“-Definition gar nicht abgedeckte – Gegenüberstellung von „Privatsphäre“ und „Öffentlichkeit“ (S. 91).

[1251] Er versucht dazu die Diskussion zum Schutzgut darzustellen und präsentiert dazu die in der Diskussion vorgebrachten „Lösungsansätze“: *right to privacy*, Sphärentheorie, „sozialwissenschaftlich orientierte Ansätze“ und Christoph Mallmanns informationelles Selbstbestimmungsrecht. Die Einordnung Westins in einem als einheitlich fingierten *right to privacy* wird ihm als Sozialwissenschaftler genauso wenig gerecht wie die von den „sozialwissenschaftlich orientierten Ansätzen“ getrennte Darstellung von Mallmanns Ansatz und die Zuordnung anderer Autorinnen in den Fußnoten als zustimmend oder ablehnend, denn sowohl Müller, Benda, Schmidt als auch Christoph Mallmann – im Gegensatz zu Otto Mallmann, der von Woertge unter die „sozialwissenschaftlich orientierten Ansätze“ gezählt wird und eigentlich in eine Liste mit Westin gehört, weil sich beide auf Goffman stützen – stützen sich in erster Linie auf die strukturalistische „Schule“ der Rollentheorie, d. h. Parsons, Merton und Luhmann.

[1252] Siehe dazu Woertge (1984, S. 84 ff.).

[1253] Woertges Auseinandersetzung damit ist absurd, wenn er etwa meint, dass immer dann, wenn die Informationsverarbeitung Vorteile für die Betroffenen habe, deren Nachteile „weniger stark ins Gewicht“ (S. 84) fielen. Mit einer solche Argumentation ließe sich eine Hausdurchsuchung rechtfertigen unter Verweis auf die Möglichkeit, damit die Unschuld der Beschuldigten beweisen zu können.

[1254] In seinen Ausführungen zum Grad der „Sensitivität“ von Informationen unterlässt Woertge aus gutem Grund jeden Hinweis auf konträre Positionen (S. 88 f.) und behauptet stattdessen für Name – „Kevin“ und „Chantal“ –, Wohnanschrift – „Berlin Hellersdorf“ – und „sog. offenkundige Daten“, etwa in „Zeitungen“, dass „jemand in der Regel kaum schwere Nachteile zu befürchten habe[]“, wenn diese verarbeitet würden. Siehe dazu auch die von den Roten Khmer durchgeführte massenweise Ermordung von Intellektuellen.

[1255] Siehe Woertge (1984, S. 91 ff.), zu den öffentlichen Stellen als Träger der Betätigungsfreiheit siehe S. 93, wobei die Ausführungen allerdings im offenkundigen Widerspruch stehen zu Woertges Ausführungen zum Vorbehalt des Gesetzes (S. 43 f.). Auch sein Verweis auf Art. 5 Abs. 1 GG geht schon insoweit fehl, als das Menschen offenkundig keine „allgemein zugängliche[] Quellen“ im Sinne des Art. 5 Abs. 1 Satz 1, 2. Hs GG sind.

[1256] Siehe dazu etwa Bull (1981b) und die Kurzfassung in Der Bundesbeauftragte für den Datenschutz (1981).

gleich ganz zu überwinden.[1257] Zu den geforderten Ergänzungen gehört die Aufnahme der Phase der Erhebung in das BDSG ebenso wie eine stärkere Ausgestaltung des Zweckbindungsgrundsatzes im Gesetz oder die Einführung einer bereichspezifischen Regelung für den Datenschutz im Medienbereich, vor allem aber eine Klarstellung des Gesetzeszwecks.[1258] In Abgrenzung zu Forderungen nach einer besseren Ausgestaltung des Datenschutzes im weiteren Sinne – etwa die Informationsmachtverteilung zwischen den Verfassungsorganen – in den Datenschutzgesetzen[1259] fordert Bull deren Beschränkung, im gleichen Atemzug jedoch auch die Einführung eines allgemeinen Informationsfreiheitsgesetzes.[1260] Rihaczek hingegen will das Datenschutz in Richtung eines allgemeinen Informationsrechts ausdehnen, etwa indem er „personenbezogene (auf die natürliche Person des Bürgers bezogene) Interessen an Daten“, und „nicht nur [...] Interessen an »personenbezogenen Daten«“ zum Anknüpfungspunkt des Rechts machen will.[1261] Fiedler will einen Schritt weiter gehen zu einer „umfassenderen, expliziten gesellschaftlichen Kontrolle und Regelung von Informationszusammenhängen als solchen“, will diesen Bereich dann allerdings auch nicht mehr als Datenschutzrecht, sondern als Informationsrecht bezeichnet wissen.[1262] Brinckmann hingegen hält das bestehende Datenschutzrecht für strukturell untauglich: Nicht nur fehle es an einer „Institutionalisierung der Beteiligung von relevanten Interessen“, sondern vor allem auch an einer „Institutionalisierung der systematischen Weiterentwicklung von Risiko- und Sicherheitsvorschriften“.[1263] Überhaupt sei das Datenschutzrecht gemessen an den Erfahrungen aus anderen Technikrechtsgebieten überaus defizitär, vor allem hinsichtlich der internen wie externen Transparenzerzeugung, d. h. einer sinnvollen „Sicherheitsanalyse“ und deren Offenlegung.[1264]

Dabei verlief die Auseinandersetzung um die Zukunft des Datenschutzes und des Datenschutzrechts keineswegs linear, sie war vielmehr geprägt von Gleichzeitigkeiten und (vielleicht) überraschenden Koalitionen, wie etwa die Dokumentation der Jahrestagung 1982 der Deutschen Vereinigung für Datenschutz zeigt.[1265] So wurde einerseits der Vorwurf erhoben, es werde mit dem Datenschutz übertrieben,[1266] vor allem durch seine zunehmende Bürokratisierung, die das Problem des exzessiven Gebrauchs von Generalklauseln im Datenschutzrecht noch verstärke.[1267] Andererseits sei die „Staatsbürokratie“ dabei, die Datenschutzgesetze auszuhöhlen, sodass nur noch eine Fassade bleibe.[1268] Die Intensität der Auseinandersetzung erkläre sich, so Klaus Hüm-

[1257] Siehe dazu etwa Rihaczek (1980), Fiedler (1981) oder Brinckmann (1982).

[1258] Es gehe nicht um den „Schutz von Daten vor Mißbrauch bei der Datenverarbeitung, sondern um den Schutz des Bürgers vor Gefahren und den Ausgleich von Schäden, die bei unangemessenem Umgang mit Informationen entstehen“, siehe Bull (1981b, S. 24).

[1259] Siehe etwa die Reste davon in § 24 Abs. 3 Berliner Datenschutzgesetz.

[1260] Siehe Bull (1981b, S. 22 f.).

[1261] Siehe Rihaczek (1980, S. 229). Sein Versuch einer „vollständigen“ Darstellung von Interessen beteiligter Akteurinnen ist hingegen untauglich, weil soziologisch uninformiert und daher extrem unterkomplex, siehe S. 231, wo nur Alice, Bob und alle Dritten voneinander unterschieden werden.

[1262] Siehe Fiedler (1981, S. 10) und zu den Problembereichen, die er mit seinem Informationsrecht abzudecken gedenkt, S. 12 f.

[1263] Wobei er damit aber gerade nicht nur Datensicherheits-, sondern auch Datenschutzvorschriften meint, siehe Brinckmann (1982, S. 161).

[1264] Siehe vor allem Brinckmann (1982, S. 163).

[1265] Siehe Gola (1983), zum letzteren schon Ronge (1981, S. 123).

[1266] Siehe Weise (1983).

[1267] Siehe Kamlah (1983). Siehe dazu die Ausführungen von Ziegler-Jung (1985), die diese Bürokratisierungstendenzen auch für Länder wie Schweden und die Niederlande nachweist, die gänzlich anderen Regelungsansätzen folgen.

[1268] Siehe Lohmar (1983).

merich, daraus, „daß es bei der Verarbeitung von Informationen wie bei den Rechtsregeln zu ihrer Begrenzung um die Ausübung von Macht geht.“[1269]

2.4.2 Das Volkszählungsurteil und seine Folgen

Das Volkszählungsurteil des Bundesverfassungsgerichts wird gemeinhin als große Zäsur verstanden.[1270] Die tatsächlichen Änderungen sind tatsächlich eher gering, wenn auch – weil das Gericht eben ein neues Grundrecht expliziert hat – sicher bedeutsam.

Das Urteil ist im wesentlichen ein Plagiat der Druckfahne der Kommentierung von Art. 1 Abs. 1 und Art. 2 GG durch Adalbert Podlech[1271] – eine Tatsache, die in der Rechtswissenschaft oft nicht bekannt, weitgehend ignoriert und teilweise absichtlich verschwiegen wird.[1272] Podlech selbst war in dem Verfahren – zusammen mit Steinmüller und Brunnstein – einer der Beschwerdeführerinnen und zusammen mit Steinmüller zugleich einer der Bevollmächtigten.[1273] Während eine Mehrzahl der Wissenschaftlerinnen – darunter mit Steinmüller, Podlech, C. Mallmann, Müller und Dammann die „Architekten“ von Datenschutztheorie und -recht – vorher das Recht auf informationelle Selbstbestimmung aus der Entscheidungsfreiheit nach Art. 2 Abs. 1 GG ableiteten,[1274] entschied sich das BVerfG für eine Ableitung aus dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[1275] und schuf damit die Basis für die heute durchaus weitverbreitete Auffassung, die informationelle Selbstbestimmung sei ein Ausfluss der Menschenwürde.[1276] Jedenfalls aber akzeptiert das BVerfG mit dem Urteil faktisch die zwei gemeinsamen verfassungsrechtlichen Anknüpfungspunkte des Datenschutzrechts – den persönlichkeitsrechtlichen und den staatsrechtlichen – in ihrer Interpretation durch eine strukturalistische

[1269] Hümmerich (1983, S. 57).

[1270] Die Zahl der Zuschreibungen ist Legion, bis hin zur Behauptung, das Gericht habe damit die „informationelle Selbstbestimmung“ selbst „entwickelt“, siehe schon Benda (1984, S. 87). Eine Auseinandersetzung mit diesen Zuschreibungen liegt – nicht nur wegen ihrer Menge – außerhalb des Rahmens dieser Arbeit. Gleiches gilt für eine tiefgehende Analyse der Bewegung gegen die Volkszählung. Siehe dazu etwa Schlink (1986, S. 233 ff.) und vor allem Massing (1987), darüber hinaus umfassend zu den historischen Kontinuitäten Aly und Roth (1984) und Steinmüller (2007).

[1271] So schon, wenn auch nicht hinsichtlich seiner Bezeichnung als Plagiat, Podlech (1984, S. 91, Fn. 14). Siehe auch umfassend Rost und Krasemann (2008), ab Minute 00:20.

[1272] So schon Roßnagel (1994, S. 228 Fn. 7). Siehe etwa von Lewinski (2014, S. 44, Fn. 176), der sie – wegen des Fehlens von Zitaten – nicht für belegbar hält und sie im übrigen eher Steinmüller zuzuschreiben scheint, an anderer Stelle – von Lewinski (2014, S. 34, Fn. 107) – aber korrekt auf Podlechs Kommentierung verweist. Anders aber Anna-Bettina Kaisers Ausführungen zur Übernahme der Konstruktion durch das Bundesverfassungsgericht, Kaiser (2009, S. 183 ff., vor allem S. 185), die von Lewinski auch zitiert.

[1273] Siehe das ausgefertigte Urteil, verkündet am 15. Dezember 1983. Das Verfahren der drei genannten Beschwerdeführer wurde unter dem Aktenzeichen 1 BvR 420/83 geführt.

[1274] Siehe etwa Steinmüller et al. (1971), Podlech (1973a) und Mallmann (1976a).

[1275] Siehe BVerfG (1983, S. 43). Siehe aber die Formulierung im Satz davor: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.“ Das ist Art. 2 GG, nicht das allgemeine Persönlichkeitsrecht!

[1276] Siehe etwa Baum (2013). Gleichwohl existiert eine Verbindung zwischen Menschenwürde und informationeller Selbstbestimmung auch in der Datenschutztheorie von Podlech, Steinmüller, Mallmann et al., insoweit sie sich alle auf die Interpretation Luhmanns stützen, nach der Menschenwürde das Ergebnis gelingender Selbstdarstellung und zugleich Ergebnis und Bedingung gelungener Selbstdarstellung ist, siehe Luhmann (1986, S. 61 und 68) – aber das impliziert gerade nicht schon die verfassungsrechtliche Anbindung der Selbstbestimmung an das Menschenwürdegebot von Art. 1 Abs. 1 GG. Podlechs Hinweis, dass mit dieser Konstruktion das Recht auf informationelle Selbstbestimmung allerdings auch direkt gegen Private gelte, ist allerdings beachtenswert, siehe Rost und Krasemann (2008), ab Minute 00:20. So explizit auch BVerfG (1991, S. 194 f.).

Theorieschule.[1277] Ganz überwinden konnte das Gericht dabei jedoch die vorwissenschaftlichen Vorstellungen – zumindest im Sprachgebrauch – nicht, auch wenn Ulrich Mückenberger das behauptet:[1278] So wird bei der vom Gericht herangezogenen Formulierung von der „Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person“[1279] schon nicht klar, ob damit Bezug auf die Gemeinschaft – wie die Begriffe implizieren – oder die Gesellschaft gemeint ist, auch weil das Gericht an anderer Stelle explizit von der „Person“ spricht, „die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt.“[1280] Wie bereits in der Vergangenheit hat das Gericht mit dieser Formulierung von der „Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit“ auch hier die Einschränkbarkeit des Grundrechts begründet, obwohl das für beide Auslegungen – als „Gemeinschaft“ und als „Gesellschaft“ – konzeptionell fehlgeht: Als liberaler Staat kann er sich eigentlich nicht – wie das etwa ein faschistischer könnte – mit der Gemeinschaft gleichsetzen,[1281] und „Gesellschaftsbezogenheit und Gesellschaftsgebundenheit“ sind keine natürlichen Eigenschaften von Menschen.[1282]

Schon kurz nach dem Urteil kam es wenig überraschend zu Streits um die Auslegung.[1283] Das BMI will einer „moderaten Interpretation“ ausgehen, die „die Anforderungen des Gerichts *berücksichtigt*, ohne die unerläßliche Funktionsfähigkeit der Verwaltung zu *gefährden*.“[1284] Das Ziel sei eine „Konkordanz zwischen dem Recht auf informationelle Selbstbestimmung, anderen

[1277] Siehe Steinmüller (1984, S. 92 f.). Insofern ist es wohl weniger ein Denkmal, das sich Benda selbst zu setzen versuchte, so – wenn auch vorsichtig – von Lewinski (2014, S. 28, Rn. 57), als vielmehr der – leider nur vorläufige – Abschluss seines langen Kampfes gegen die Sphärentheorie, siehe Benda (1974) und die Tatsache, dass er diesen Beitrag an Müller, den er dort zitierte, schickte mit der Bemerkung, damit die Fixierung auf die Sphärentheorie in der rechtswissenschaftlichen Debatte überwinden zu können, siehe Rost (2012a), ab Minute 41:00. Siehe dazu auch Benda (1984, S. 88), Podlech (1984, S. 91 f.) und die Ausführungen des Berichterstatters im Volkszählungsverfahren, Hermann Heußner (1987, S. 118 f.). Auf eine andere Auseinandersetzung, die im Urteil auch nicht explizit angesprochen wird, aber in der sich das Gericht in seinen Entscheidungsgründen eindeutig positioniert, verweist Podlech (1984, S. 85 ff., vor allem S. 88 f.): der Versuch der bundesdeutschen Sicherheitsbehörden, ein umfassendes Kontroll- und Überwachungssystem aufzubauen, und der jahrzehntelange Kampf dagegen. Und trotzdem sich das Gericht in seiner Entscheidung auf die strukturalistische Theorieschule stützte, hat die individualistische langfristig die Oberhand behalten: Indem sich die sogenannten kritischen Datenschützerinnen um das BVerfG und das Urteil scharten, um beide gegen die Angriffe vor allem aus dem Sicherheitslager, aber auch aus der Wirtschaft, zu verteidigen, haben sie gerade die individualistische Phrasen und Konstruktionen des BVerfG, etwa dass das Grundrecht „insoweit die Befugnis des Einzelnen [gewährleistet], grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ BVerfG (1983, S. 43), mehr und mehr zu Fetischen erhoben und als Selbstzwecke imaginiert. Und damit haben sie dann in der Folge jeden Widerstand gegen diese individualistische Lesart nicht nur aufgegeben, sondern diese Lesart sogar zu ihrer ureigenen gemacht.

[1278] Siehe Mückenberger (1984, S. 4 ff.). Vielleicht liegt das daran, dass auch Mückenberger sich davon nicht ganz lösen kann oder will. Darauf deuten jedenfalls die Ausführungen auf S. 17 hin, die er zur Rettung der „Privatheit“ versucht – wenn nicht als „Sphäre“, „so doch in einem »geschützten« Interaktionsgefüge“, das es „abzuschirmen“ gelte.

[1279] Siehe BVerfG (1983, S. 44) mit Nachweisen aus der Rechtsprechung des BVerfG.

[1280] Siehe BVerfG (1983, S. 41).

[1281] Siehe dazu die Hinweise bei Mückenberger (1984, S. 7, vor allem Fn. 37).

[1282] Das heißt nicht, dass sich mit einem Verweis auf „Gesellschaft“ und gesellschaftliche Erfordernisse nicht eine Einschränkbarkeit des Grundrechts formulieren ließe, siehe für einen solchen Ansatz etwa Ronge (1981), sondern dass Gesellschaft nicht „natürlich“ ist. Eine Verweisung auf Gesellschaft würde daher vielleicht schon die Einschränkbarkeit als solche, jedenfalls aber die Bedingungen der Einschränkung als gesellschaftlich konstruiert und damit deutlich auch als gesellschaftlich aushandelbar markieren.

[1283] Siehe zu den Typen von gesetzgebungspolitischen Reaktionen – das Weiter-so, das Alles-neu und der „gesetzesförmliche[] Grundrechtsleerlauf“ – Denninger (1985, S. 215 f.) und Denninger (1987, S. 127 ff.). Der Streit hat sich mit der Zeit auch nicht gelegt, siehe dazu etwa Simitis (2000).

[1284] Siehe Bundesministerium des Innern (1984, S. 282 f.) – die DuD dokumentiert damit eine Vorlage des BMI an den Innenausschuss des Deutschen Bundestages. Hervorhebung durch den Autor. Das BMI widerlegt damit

verfassungsrechtlich geschützten Gütern und *den Gegebenheiten der Praxis*“[1285] – das ist nicht „moderat“, sondern genau das Gegenteil von dem, was das Bundesverfassungsgericht im Urteil erklärte. Deutlicher kann das BMI seine Vorstellung von Grundrechten nicht äußern: Sie stellen keine Anforderungen an die Praxis, sondern sie können allenfalls gelten, wenn sie die Praxis nicht ändern![1286] Zumindest erklärt das die nachfolgenden Versuche, das Datenschutzrecht strukturell zu unterminieren.[1287]

Auf der anderen Seite steht – ebenso wenig überraschend – der ehemalige Gerichtspräsident Benda, der aus dem Urteil fünf erforderliche Ergänzungen des Datenschutzrechts folgert: Einbeziehung der Phase der Erhebung in den Schutzbereich, „Beschränkung des Ausmaßes der Erhebung und des Austauschs von Daten, nicht lediglich eine Verhinderung von Mißbräuchen“, Auskunftsrechte der Betroffenen auch im Sicherheitsbereich, Verankerung des Zweckbindungsprinzips sowie die Mitteilung von Zweck und Adressaten bereits bei der Erhebung von Informationen.[1288] Auf den Aspekt der Überwindung der Fixierung auf „Missbrauch“ geht auch Steinmüller ein und identifiziert im Urteil einen Schwenk zu einer allgemeinen „Gebrauchsregelung“, den er fast schon euphorisch begrüßt.[1289] Zugleich warnt er aber auch vor der nur teilweisen Durchsetzbarkeit von Datenschutz im Recht: Es stünden „sehr große organisierte Interessen gegen die Betroffenen“, und das Urteil könnte ein Vertrauen erzeugen, das der Realität nicht standhalte.[1290]

Dieser grundsätzliche Streit um die „richtige“ Interpretation des Bundesverfassungsgerichtsurteils und insbesondere die daraus zu ziehenden Schlussfolgerungen sowohl für die neueren technischen Entwicklungen – einerseits die Einführung und Durchsetzung des Personal Computers, andererseits die zunehmende Vernetzung und die Entstehung vernetzter Netze – prägten einen wesentlichen Teil der Diskussion in der zweiten Hälfte der 80er und zu Beginn der 90er Jahre. Hinzu kamen die damals großen gesellschaftlichen Auseinandersetzungen – die neuen sozialen Bewegungen, wahrscheinlich vor allem die Umweltbewegung, der „Kampf gegen die organisierte Kriminalität“ sowie große öffentliche Streitgegenstände von der Startbahn West über Wackersdorf bis zu Tschernobyl – und der Umgang des Staates als „Informationsmachtzentrale“ damit – sowohl hinsichtlich der Informationseingriffe wie der Informationskontrolle –, die die Berufsverbote und die Anti-Terror-Gesetze der 1970er Jahre als gesellschaftliche Bezugspunkte der Datenschutzdebatte ersetzten oder zumindest in den Hintergrund drängten.[1291] Auch in

zugleich die Behauptung, dass „Fehl-, Über- aber auch Unterinterpretationen [...] nur schwer möglich sein“ würden, siehe Bäumler (1984, S. 361).

[1285] Siehe Bundesministerium des Innern (1984, S. 285). Hervorhebung durch den Autor.

[1286] Siehe dazu auch die Einschätzung von Simitis (1984, S. 399), dass das Grundgesetz nicht Verarbeitungsfreiheit garantiere, sondern gerade „Verarbeitungsbarrieren“ begründe.

[1287] Siehe zu den Entwicklungen in dieser Richtung in den ersten zehn Jahren nach dem Urteil Deutsche Vereinigung für Datenschutz (1994). Denningers dritter Typ hat deutlich gewonnen.

[1288] Siehe Benda (1984, S. 90).

[1289] Siehe Steinmüller (1984, S. 93). Gleiches gilt für die Gesellschaft für Informatik, siehe Gesellschaft für Informatik (1984, S. 112). Auernhammer, der für das Datenschutzrecht – und damit eine mögliche Novellierung – zuständige Referent im BMI, will hingegen nicht nur am Missbrauchsbezug festhalten, sondern den Umfang der Änderungen auch sonst klein halten, siehe Auernhammer (1984).

[1290] Siehe Steinmüller (1984, S. 96). Es besteht der dringende Verdacht, dass Steinmüller recht behalten hat, sowohl im Hinblick auf die Stärke der Gegeninteressen als auch im Hinblick auf die Vertrauenserzeugung und dessen anschließende Enttäuschung. Leider gibt es gerade zu letzterem nur sehr wenig Forschung, siehe etwa Hallinan et al. (2012); zur Frage der Diskrepanz zwischen den geweckten Erwartungen und der Realität – sowohl in Bezug auf das Datenschutzrecht selbst als auch in Bezug auf das Verhältnis zwischen Datenschutzrecht und Wirklichkeit – ist dem Autor keine Veröffentlichung bekannt.

[1291] Siehe etwa „Testfall Startbahn West“, an der auch Podlech mitgeschrieben hat, aber auch Denninger (1985), Bäumler (1987), Schwan (1987), Kauß (1989). Die Wende und der Beitritt der DDR zur Bundesrepublik haben

den englischsprachigen Ländern gab es keine großen Umbrüche in der Diskussion – in der die verschiedenen Diskussionsstränge weitgehend parallel nebeneinander liefen, ohne sich groß zu beeinflussen –, abgesehen vielleicht vom Aufkommen der „Surveillance Studies“ zu Beginn der 90er Jahre und einer Zunahme an Arbeiten zu Fragen der Governance, rechtsvergleichenden Arbeiten und Untersuchungen zur Möglichkeit der Übertragbarkeit von Regelungsansätzen. Eine relativ starke Zunahme gab es bei Arbeiten, die sich mit der Technikgestaltung beschäftigten, insbesondere zu Verfahren und Modellen, während es im Bereich der „Kerninformatik“ in dieser Zeit vor allem um Anonymisierung und Anonymität und die dafür notwendigen kryptographischen Grundlagen ging.

Auf der einen Seite unternimmt es der damalige Bremische Landesdatenschutzbeauftragte Alfred Büllesbach, vor dem Hintergrund der sich zu dieser Zeit vollziehenden technischen Entwicklung eine zusammenfassende Betrachtung von Datenschutzproblem und Datenschutzrecht vorzulegen,[1292] um die stattfindende Reformdiskussion zu beeinflussen, und lehnt dabei das auf Luhmanns Vorarbeiten basierende Bedrohungsmodell des Datenschutzes zugunsten des von Rüpke ausgearbeiteten ab.[1293] Auf der anderen Seite versucht Steinmüller, den Datenschutz theoretisch und praktisch zu verbreitern, indem er dessen Schutz der Handlungsfreiheit ausdehnt auf das Ziel der Schaffung von (neuen) Handlungsmöglichkeiten für Betroffene von Informationssystemen – „über die löcherigen Datenschutzgesetze“ hinaus –, vor allem in Unternehmen.[1294] Den Hintergrund, vor dem Steinmüller die entstehenden Probleme analysiert und Lösungsvorschläge unterbreitet, bilden dabei das Verständnis des Computers als allgemeine Medien- und zugleich (Entscheidungs-)Rationalisierungsmaschine, sein möglicher Gebrauch als „Universalkontrollmittel“ sowohl für Menschen wie für Dinge und Prozesse als „»Fabriken« für Machtmöglichkeiten“, die absehbare Entwicklung hin zum „computer integrated manufacturing“ – heute „Industrie 4.0“ – bei gleichzeitiger Übertragung von (unbezahlter) Arbeit auf Kundinnen („Schattenarbeit“) – das gleiche Geschäftsmodell im Internet wird heute als AAL-Prinzip bezeichnet: „Andere arbeiten lassen“ (Andreas Weigend) – sowie die allgemeine Tendenz zu (eng gekoppelten) „Großtechnologien“.[1295] Aber nicht nur Büllesbach und Steinmüller, sondern auch Simitis fordert eine Weiterentwicklung des Datenschutzrechts, wobei seine Hauptkritikpunkte an den bestehenden rechtlichen Regelungen das Primat der Selbstkontrolle der verantwortlichen Stelle – und damit deren Fähigkeit, „ihre bisherigen Verarbeitungsprozeduren [...] beizubehalten“ –, die Konstruktion der Datenschutzgesetze als „Auffanggesetze“ – oder jedenfalls deren erfolgreiche Umdefinition in Auffanggesetze in der öffentlichen und juristischen Debatte – und die grundlegende Ungeeignetheit der Einwilligung in vielen Handlungskontexten sind.[1296] Dem

relativ wenig Einfluss auf die Diskussion gehabt – die bundesdeutsche Datenschutzrechtskonzeption ist, wie in anderen Rechtsbereichen auch, auf die neuen Bundesländer übertragen worden, während zugleich die neuen Datenschutzaufsichtsbehörden analog zu den bereits bestehenden organisiert wurden.

[1292] Siehe Büllesbach (1985). Als Zusammenfassung des Diskussionsstandes ist die Arbeit sehr gut, sie bringt jedoch wenig Neues.

[1293] Siehe Büllesbach (1985, S. 109 ff.) mit Verweisen auf Podlech, Steinmüller, Müller und – etwas überraschend – Otto Mallmann auf der einen und Rüpke auf der anderen Seite, beides allerdings mit sehr schwachen Argumentationen.

[1294] Siehe dazu und zum folgenden Steinmüller (1985a), er wird das dann später „Betroffenenschutz“ nennen, siehe Steinmüller (1987, S. 64). Kritisch zur Lösbarkeit des Problems Kubicek (1986).

[1295] Siehe zu diesen Entwicklungen auch umfassend Kubicek und Rolf (1985).

[1296] Siehe Simitis (1986, S. 23, 24, 35). Seine Darstellung der „Konstituierung“ von Personengruppen in der und durch die Datenverarbeitung und der „weitere[n] Beurteilung des Betroffenen an der Zugehörigkeit zu der einzelnen Gruppe“ nimmt dabei die Diskussion um das „panoptic sort“ (Gandy) und das „social sorting“ (Lyon) vorweg, siehe Simitis (1986, S. 29), geht jedoch selbst auf Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil zurück, siehe BVerfG (1983, S. 48).

schließt sich Bull im wesentlichen an und fordert eine Neukonzeption des Datenschutzrechts als „Informationsrecht“, das „von den betroffenen *Interessen*“ ausgehen müsse und nicht allein „eine *Abwägung* der widerstreitenden Belange“ fordern dürfe, wobei er dann allerdings sehr schnell sehr konkret wird und etwa fordert festzulegen, welche Daten über Beschäftigte erhoben und verarbeitet werden dürften.[1297]

Gerade dieser Art von – tendenziell – falscher Konkretheit versuchen Steinmüller und Co. mit einer breit angelegten Diskussion im Rahmen des August-Bebel-Kreises, einem SPD-nahen Arbeitskreis von Wissenschaftlerinnen, Künstlerinnen und Politikerinnen in der zweiten Hälfte der 80er Jahre, über die „sozialökologischen Handlungsspielräume“ in der „verdatet[en] und vernetzt[en]“ Informationsgesellschaft entgegenzutreten.[1298] Sie identifizieren Informationstechnik dabei als grundsätzlich gestaltbar und daher gestaltungsbedürftig,[1299] warnen jedoch zugleich vor grundlegenden Eigeschaften von Datenverarbeitungssystemen, in denen „alles in Daten“ abgebildet werde und damit „[s]oziale Prozesse [...] im Prinzip so berechenbar und beherrschbar gemacht werden wie technische Prozesse.“[1300] Es gebe zwei tendenziell mögliche Entwicklungsrichtungen: Systeme, über die Individuen „wie bei anderen Werkzeugen frei verfügen könnten“, und Systeme, bei denen sie das nicht könnten, sondern die als „Organisations-, Steuerungs- und Kontrollinstrumente“ den Interessen Dritter, etwa Arbeitgeberinnen oder Anbieterinnen dienten,[1301] denn die „gesellschaftlich verwirklichte Technik bestimmt den Spielraum möglichen Verhaltens der Institutionen, Gruppen und Mitglieder der Gesellschaft.“[1302] Um damit gesellschaftlich umgehen zu können, bedürfe es aber einer anderen informatischen Bildung, die gerade nicht in einer Programmiererinnenausbildung bestehe, sondern in der Vermittlung der Fähigkeit zur sozialen Beherrschung der Technik.[1303]

Während die Debatte in der Rechtsinformatik im Allgemeinen und im Datenschutzbereich im Besonderen vordergründig ein gewisses Niveau erreicht haben zu schien, mangelte es ihr offensichtlich an der Fähigkeit oder der Macht, die Erkenntnisse in einer Form in die allgemeine juristische Debatte einzubringen, die verhindert, dass bereits erreichte Einigungen – oder jedenfalls akzeptierte Differenzen – über zugrunde gelegte Annahmen und gezogene Schlussfolgerungen über das Datenschutzproblem und den Ansatz zu seiner gesellschaftlichen – und insbesondere rechtlichen – „Lösung“ von weiteren Debattenteilnehmerinnen einfach ignoriert oder gar für nichtexistent erklärt werden können. Die Folge davon zeigt ein Beitrag von Horst Ehmann.[1304] Der Autor muss, um den von ihm identifizierten Gegensatz zwischen einem „absoluten Informationsschutz[] und vollkommener Informationsfreiheit“[1305] zugunsten der „Informationsfreiheit“ „lösen“ zu können, sowohl die inhaltlichen Positionen der Gegenseite falsch wiedergeben, mit „Klassenkampf“- und „Radikalen“-Rhetorik operieren, die Erkenntnisse, die im Zuge der Auseinandersetzungen gewonnen wurden, ignorieren als auch Individuen und private Organisationen in eins setzen und dann beide als Individuen – als „Mensch“ oder „Bürger“ – behandeln. Sein Menschenbild, das sich unter anderem darin äußert, dass Ehmann von Frauen verlangt, dass

[1297] Siehe Bull (1987, S. 180 f.), Hervorhebungen im Original.
[1298] Siehe Steinmüller (1988b).
[1299] Siehe Steinmüller (1988a, S. 29 ff., 33 f.) und Finckh (1988, S. 198).
[1300] So Kubicek (1988, S. 94 f.).
[1301] Siehe Kubicek (1988, S. 95 f.), der damit fast schon die Zweiteilung von offenen Systemen (oder Plattformen) und „Walled Gardens“ vorwegnimmt.
[1302] Podlech (1988, S. 118).
[1303] Siehe Schnepel und Steinmüller (1988, S. 186 ff.).
[1304] Siehe Ehmann (1988). Das gleiche gilt im wesentlichen auch für seine späteren Beiträge Ehmann (1998) und Ehmann (1999).
[1305] Siehe Ehmann (1988, S. 232).

sie ihre Schwangerschaft gegenüber „dem Vater“, d. h. nicht einmal gegenüber ihren Eltern – und das 1988! – bekanntzugeben habe, und gleichzeitig das Bankgeheimnis der Verfolgung von Steuerhinterziehung vorrangig hält,[1306] ist sowohl vorwissenschaftlich, gesellschaftspolitisch reaktionär als auch von einer Unterordnung des Menschen unter die Interessen der Wirtschaft geprägt. Die Argumentation der Arbeit basiert wesentlich auf einer Zuschreibung von personalen Eigenschaften an Organisationen, um dergestalt Interessen von Organisationen als „Gegeninteressen“ dem Datenschutzinteresse der Betroffenen als gleichwertig gegenüberstellen zu können.[1307] Während er nun die „Bürger“ mit den Organisationen gleichsetzt und dabei die Organisationen vermittelt über den Strohmann der „Bürger“ vor den Folgen von „Informationsschutz“ und „Geheimnisschutz“ schützen will,[1308] versucht er andererseits, den Schutzbereich des allgemeinen Persönlichkeitsrechts auf etwas, das sich „gegenständlich verkörpert“ habe, zu beschränken.[1309] Durch die ganze Arbeit zieht sich mmer wieder die Konstruktion einer als abgeschlossen verstandenen „Privatsphäre“, um deren Schutz es dem Datenschutzrecht gehen solle, etwa im Gegensatz zur „Sozialsphäre“, die dann für ungeschützt erklärt werden kann.[1310] Trotz seiner umfassenden Ausführungen zur soziologischen Konstruktion der Selbstbestimmung des Menschen vermeidet er es konsequent, diese Selbstbestimmung als *Selbstbestimmung* zu betrachten, und setzt sie stattdessen mit einem „Geheimnisbereich“ gleich, den er dann angreift.[1311] Und immer dann, wenn es um Interessen gegen wirtschaftlich mächtige Akteure geht, will Ehmann diese nicht als rechtlich geschützt ansehen, sondern setzt auf „ethische Prinzipien“ oder fordert einen „möglichst schonend[en]“ Umgang mit personenbezogenen Informationen.[1312] Dabei werden „Wirtschaftsverkehr“ und „wirtschaftliche Erwägungen“ als letztbegründend und damit über den Grundrechten stehend angenommen.[1313] Um seine Argumentation zu „stärken“, legt er ihr sachlich falsche Behauptungen zugrunde: So sollen private Stellen nicht der Zweckbindung bei der „Datennutzung“ unterworfen werden, „weil bei privaten Stellen auch nicht solche *Massen* von Daten gesammelt, gespeichert und genutzt werden können.“[1314] Während Ehmann an mehreren Stellen die „*soziologischen* Erkenntnisse“ als „im wesentlichen als zutreffend“ bezeichnet, behauptet er jeweils gleichzeitig, aber ohne an irgendeiner Stelle dafür eine Begründung anzugeben, dass die daraus „gezogenen *juristischen* Folgerungen“ nicht akzeptiert werden dürften.[1315] Stattdessen legt er eine offensichtlich vormoderne Theorie zugrunde, die den Menschen allenfalls in Gemeinschaften, nicht jedoch auch in Gesellschaften zum Gegenstand hat und ihn nicht als gesellschaftlich geformt und bedingt annimmt, sondern sein Sozialverhalten in seiner „Natur“

[1306] Siehe zum Menschenbild Ehmann (1988, S. 329, aber auch 379 f.), zur Informationspflicht gegenüber dem Vater Ehmann (1988, S. 291) und zum Verhältnis von Bankgeheimnis und Steuerhinterziehung Ehmann (1988, S. 279).

[1307] Siehe etwa Ehmann (1988, S. 287). Siehe auch Ehmann (1988, S. 325) zur Nichtunterscheidung der Zweckbindung bei Organisationen und Menschen sowie zur Nichtunterscheidung zwischen tatsächlicher und rechtlicher Zweckbindung – das strafrechtliche Verbot der Körperverletzung schützt auch nicht vor der anfliegenden Kugel!

[1308] Siehe Ehmann (1988, S. 373). Dabei adressiert das Datenschutzrecht gar nicht „Bürger“, sondern Organisationen im soziologischen Sinne, die nur eben – wie bei freien Berufen nicht unüblich – *auch* als natürliche Personen im juristischen Sinne auftreten können.

[1309] Siehe Ehmann (1988, S. 252 f., 304 ff.).

[1310] Siehe beispielhaft Ehmann (1988, S. 291).

[1311] Siehe Ehmann (1988, S. 372 f.).

[1312] Siehe Ehmann (1988, S. 237 ff., 297, 333).

[1313] Siehe etwa Ehmann (1988, S. 272 ff.).

[1314] Siehe Ehmann (1988, S. 322).

[1315] Siehe Ehmann (1988, S. 330, 332, 333, 334, *passim*).

verortet,[1316] oder er verweist auf eine ebenso ominöse wie begründungsfreie „Lebensklugheit“[1317] und „uralte Klugheits- und Erfahrungsregeln“[1318] als Verarbeitungsrechtfertigung. Ehmanns Behauptung, das Recht auf informationelle Selbstbestimmung wolle den Menschen als „Intimperson“ schaffen – und nicht als „Sozialperson“ –,[1319] widerspricht sowohl dem – von Ehmann selbst zitierten – Begründungszusammenhang dieses Rechts als auch der – auch von Ehmann angeführten – Luhmannschen Persönlichkeitskonstruktion „im sozialen Verkehr, indem auf seine Selbstdarstellung, sei es durch Konsens, sei es durch Dissens, eingegangen wird“,[1320] insbesondere insoweit Ehmann daraus schließen will, „daß der Wert des im sozialen Verkehr gewonnenen Persönlichkeitsbildes von der konsequenten und zuverlässigen Information durch die betroffenen Personen abhängt, die nicht durch selbstbestimmte Informationsbeschränkung *verfälscht* worden sind.“[1321] Ehmann verwechselt hier offensichtlich – absichtlich oder unabsichtlich – Luhmanns Hinweis auf die Konsistenz der Selbstdarstellung – „konsequent, erwartbar, zuverlässig“[1322] – mit einer Wahrhaftigkeit und sogar Vollständigkeit von Selbstdarstellung im Rollenspiel.

Ähnlich argumentiert Lorenz Gräf Anfang der 90er Jahre in seiner Dissertation.[1323] Auch er setzt Privatheit an den Anfang und behauptet dann, Datenschutz diene dem Schutz von Privatheit,[1324] um dann „herauszufinden, wodurch private Zustände gekennzeichnet sind, was die Funktionen von Privatheit sind und mit welchen Mechanismen Menschen ihre Privatheit aufbauen und erhalten.“[1325] Privatheit ist dabei für Gräf in erster Linie ein Zustand von Geheimhaltung und Nichtwissen, zugleich aber auch alles und jedes,[1326] ohne dass er daraus die Konsequenz zieht, den Begriff der Privatheit als überholt oder untauglich zu verwerfen.[1327] Nach einem Überblick über die verschiedenen Privatheitstheorien[1328] kommt er zu einer ausschließlich personenfixierten Definition von Privatheit als „Zustand, in dem die Lebensäußerungen einer Person relativ zu nicht mitgemeinten anderen Personen sozial folgenlos sind“,[1329] die das Verhältnis zwischen Individuen oder Gruppen und Organisationen gar nicht in den Blick nimmt, um diese Privatheit dann in „Zustände“ und „Funktionen“ zu trennen.[1330] Hinzu kommt, dass er das informationelle Selbstbestimmungsrecht falsch als „Eigentumsrecht“ sieht, indem er behauptet, dass es wie ein Eigentumsrecht funktioniere,[1331] und dass er moderne Informationsverarbeitung nicht versteht und daher glaubt, es gebe Informationen, die „aus Sicht des Persönlichkeitsschutzes

[1316] Siehe Ehmann (1988, S. 232 f. und Fn. 2).
[1317] Siehe Ehmann (1988, S. 326).
[1318] Siehe Ehmann (1988, S. 328).
[1319] Siehe Ehmann (1988, S. 335 f.).
[1320] Siehe Luhmann (1986, S. 61), zitiert nach Ehmann (1988, S. 335), der sich auf die erste Auflage von 1965 bezieht.
[1321] Ehmann (1988, S. 335).
[1322] Luhmann (1986, S. 61).
[1323] Siehe Gräf (1993).
[1324] Siehe Gräf (1993, S. 5).
[1325] Gräf (1993, S. 7).
[1326] Siehe Gräf (1993, S. 11, 13).
[1327] Siehe dazu Pohle (2016a).
[1328] Siehe Gräf (1993, S. 11 ff.). Er betrachtet Warren/Brandeis und Prosser – geht aber nicht auf Bloustein ein –, Simmel, Goffman, Halmos, Westin, Laufer/Wolfe, Müller, Altman, Marshal und Padersen sowie Rubenfeld und Chlapowski, trotz seiner Vollständigkeitsbehauptung jedoch nicht Beardsley, Rule, Foddy und Finighan, Gavison oder Allen.
[1329] Siehe Gräf (1993, S. 39), eine „dyadische Interaktionskonstellation, also eine Situation, die von zwei Personen geteilt wird“ (S. 305).
[1330] Siehe Gräf (1993, S. 41 ff., 77 ff.). Sowohl die Zustände wie die Funktionen sind die gleichen wie bei Westin (1967), aber nur bei den Zuständen weist der Autor darauf hin, dass sie „sich an den Unterscheidungen Westin“ „orientieren“ (S. 41, Fn. 18).
[1331] Siehe Gräf (1993, S. 173).

an und für sich belanglos sind“, und als Beispiel für solche „belanglosen“ Informationen „äußere körperliche Merkmale“ nennt.[1332] Wie Ehmanns basiert auch Gräfs Argumentation zu den Gefährdungen auf – schon damals widerlegten – falschen Behauptungen, etwa dass „[u]nsichtbar und unzugänglich [...] die internen Zustände eines Menschen [seien] und das, was der Mensch exklusiv (d. h. in Abwesenheit anderer [Menschen, denn nur darüber spricht Gräf]) wahrnimmt oder tut“[1333] oder dass „aus dem Normalvollzug der Verwaltung keine Gefahr [drohe], sondern aus dem aus privaten Antrieben motivierten Mißbrauch.“[1334] Seine „Gefahrenanalyse“ muss darum auch scheitern.[1335] Auch scheint Gräf weder die Funktionsweise von Grundrechten noch das Rechtsstaatsprinzip zu verstehen, wenn er sich darüber mokiert, dass das BVerfG das Recht auf informationelle Selbstbestimmung zwar als „allgemeines Abwehrrecht konstituiert [habe], es aber im Bereich des öffentlichen Rechts entwertet, indem es Einschränkungen durch Gesetze zuläßt.“[1336] Es kann sich aber auch um eine direkte Folge seiner Konstruktion der Privatheit als quasi gesellschaftsfreiem Zustand handeln, das er gerade dadurch bedroht sieht, dass diese Privatheit – oder korrekter: das Recht auf informationelle Selbstbestimmung – Gegenstand „kollektive[r] Regelungen“ wird.[1337]

Im Gegensatz dazu steht Bernhard Hoffmanns Arbeit zur Zweckbindung und der Funktionen, die sie im Rahmen des prozeduralen Regelungsansatzes, den der Datenschutz im bundesdeutschen Datenschutzrecht gefunden hat, erfüllen soll,[1338] der die historische Konstruktion dieses Prinzips ernst nimmt und ihr nicht einfach seine eigene Vorstellung überstülpt. Seine Analyse beschränkt sich dabei auf die Erforderlichkeit des Zweckbindungsprinzips für die „Wahrung des ursprünglichen Erhebungskontexts“ und insbesondere für die Schaffung „wohlgeordnete[r], transparente[r] und kontrollierbare[r] Strukturen“.[1339] Hoffmann identifiziert Zwecke einerseits als strukturbildend, indem sie Bereiche definieren und mithin die Grenzen zwischen den Bereichen, die zur Informationsflusskontrolle genutzt werden können.[1340] Andererseits dienen sie, so Hoffmann, der Bestimmung der Menge der für die Zweckerreichung, also innerhalb der Bereiche, funktional äquivalenten Handlungsmöglichkeiten und Mittel.[1341] Datenschutzrechtlich handelt es sich dabei um die Bestimmbarkeit der Geeignetheit, wobei die Setzung von Zwecken den Raum aller überhaupt möglichen Handlungen und Mittel sowie ihrer Wirkungen in er-

[1332] Siehe Gräf (1993, S. 178). Wahrscheinlich meint er damit Hautfarbe, Nasenform und Behinderungen... Siehe auch die Ausführungen auf S. 283 ff.

[1333] Gräf (1993, S. 195) und die nachfolgenden Ausführungen.

[1334] Gräf (1993, S. 210). Damals schon bekannte Gegenbeispiele finden sich etwa bei Steinmüller (1979a), Bölsche (1979) oder Kauß (1989).

[1335] Extrem wird dieser Unsinn, wenn er aneinandergereiht wird: „Die Vertraulichkeit der Arzt-Patienten-Kommunikation [Schutzgutunterstellung!] ist nicht durch die sekundäranalytische Verwendung von Abrechnungsdaten verletzbar [Allaussage, weil nicht auf einen bestimmten oder bestimmte Datenverarbeiter eingeschränkt]. Wie bei unseren Überlegungen immer wieder deutlich wurde, ist erst die Weitergabe geschützter Informationen an Personen [gefährliche Datenverarbeiter, wie Krankenkassen, fallen durch diese Beschränkung auf Personen heraus], die in irgendeiner Beziehung zu dem Patienten stehen, für die also die Informationen überhaupt Relevanz haben, als Verletzung von Privatheit zu bezeichnen. Bezogen auf die Arzt-Patient-Kommunikation sind relevante Personen in diesem Sinne Freunde, Bekannte, Nachbarn, Arbeitskollegen oder Arbeitgeber [sowie Polizeien, Geheimdienste, Gerichte, Versicherungen, Werbeunternehmen, die er leider vergisst].“ (S. 239).

[1336] Siehe Gräf (1993, S. 182).

[1337] Siehe Gräf (1993, S. 182).

[1338] Siehe Hoffmann (1991). Siehe zur Einordnung, zur Kritik und zum nachfolgenden Pohle (2015b).

[1339] Hoffmann (1991, S. 127 und 26).

[1340] Hoffmann (1991, S. 25).

[1341] Hoffmann (1991, S. 81), mit Verweis auf Luhmann (1964a, S. 109).

wünschte und unerwünschte trennt.[1342] Zugleich eröffnet die Zwecksetzung die Möglichkeit, die grundsätzlich erwünschten Handlungsalternativen und Mittel sinnvoll miteinander vergleichen zu können,[1343] so etwa zur Unterscheidung zwischen erforderlichen und nicht erforderlichen Handlungen und Mitteln. Auf dieser Basis kann abschließend die Angemessenheit der Handlungen und Mittel adressiert werden. Mit der Zweckbindung, der „Gewährleistung einer ausschließlich zweckbestimmten Verwendung“,[1344] wird dann Kongruenz von Sollen und Sein sichergestellt. Die Funktion des Zweckbindungsprinzip ist demnach die Erzeugung von Kontrollierbarkeit der Informationserhebung, -verarbeitung und -nutzung sowie der dabei verwendeten technischen wie nicht-technischen Mittel, indem es wohlgeordnete Organisationsstrukturen und Prozesse erzeugt, die zugleich transparent gemacht werden können – den Organisationen selbst, vor allem jedoch den Betroffenen und den Aufsichtsbehörden. Zwar ist Hoffmanns Arbeit in der Literatur hin und wieder zitiert worden,[1345] jedoch wird dabei fast nie auf die Funktion des Zweckbindungsprinzips eingegangen, und wenn, dann nur ab der abstrakten Ebene, nämlich dass sie die grundsätzlich zweckfrei mögliche Informationsverarbeitung zu beschränken vermag.[1346]

2.4.3 Die englischsprachige Debatte zwischen Philosophie, Recht und Governance

Die nicht-informatische englischsprachige Debatte zwischen Mitte der 80er und Mitte der 90er Jahre war geprägt von einer Zweiteilung – einerseits der Fortführung der grundsätzlichen Auseinandersetzung darum, was unter dem *privacy*-Problem zu verstehen sei und wie es gelöst werden müsse, und andererseits wurde eine durchaus ansehnlichen Zahl von rechts- und politikvergleichenden Arbeiten vorgelegt.

Ferdinand Schoeman, dessen Arbeiten durchaus häufig rezipiert werden – wahrscheinlich aber vor allem, weil er sie als „philosophisch“ ausweist, und sie damit als „Grundlagenwerke“ erscheinen –, unterscheidet drei Formen von *privacy*: den Zustand, die Kontrolle über den Zustand sowie das Recht auf Kontrolle über den Zustand.[1347] Die weite Rezeption auch heute ist insofern überraschend, als dass Schoemann aus seiner *privacy*-Betrachtung explizit gerade die sozialen Beziehungen ausschließt, um die es in der heutigen Diskussion vor allem geht: den Bereich der Wirtschaft sowie den staatlichen Bereich.[1348] Stattdessen wolle er sich beschränken auf „the less formal but possibly more important domains of social life, including the whole spectrum of social interaction“,[1349] also ausschließlich interpersonale Beziehungen. Unabhängig davon sind Schoemans „spheres of life“ nichts anderes als Goffmans Rollen mit „implicit privacy norms built in“, deren Zweck „freedom from overreaching social control“ sei.[1350]

Eine solche Selbstbeschränkung nimmt auch Anita Allen vor und vertritt eine reduktionistische *privacy*-Konzeption, in der *privacy* ein Zustand ist, „a degree of inaccessibility of persons, of their

[1342] Hoffmann (1991, S. 46).
[1343] Hoffmann (1991, S. 50).
[1344] Hoffmann (1991, S. 21).
[1345] Siehe jüngst von Grafenstein (2015).
[1346] Siehe etwa Kutscha (1999, S. 157).
[1347] Siehe Schoeman (1984b, S. 199) und Schoeman (1984c, S. 2 ff.).
[1348] Am deutlichsten wird dies in seinem 1992 erschienenen Buch „Privacy and social freedom“, siehe Schoeman (1992, S. 22), mit der Begründung, ihre Behandlung „may bias our understanding“.
[1349] Schoeman (1992, S. 22).
[1350] Siehe Schoeman (1992, S. 9 f.). Diese Sphären mit den eingebauten *privacy*-Normen sind ziemlich sicher auch die Grundlage für Nissenbaums „contextual integrity“, siehe Nissenbaum (2004) und Nissenbaum (2010), vor allem aber Nissenbaum (1998, S. 583, Fn. 57). Die Idee sei einfach „in the air“ gewesen, so Barth et al. (2006, S. 2) – eher wohl „in the library“...

mental states, and of information about them to the senses and surveillance devices of others.“[1351] Daneben nutzt sie den Begriff der „private sphere“ für den Haushalt und verweist darauf, dass es sich dabei auch um eine vermachtete Struktur handelt – zu Ungunsten der Frauen.[1352] Für *privacy* in der Öffentlichkeit setzt sie *privacy* mit Abgeschiedenheit und Anonymität gleich.[1353] Da in allen Fällen immer nur „others“ die Angreiferinnen sind, ist Allens *privacy*-Konzept eines von Asozialität in einem ganz umfassenden Sinne: *privacy* kann es nur für diejenige geben, die niemanden um sich herum hat – alles andere ist schon nur noch aufgegebene *privacy*.[1354]

Der dritte im Bunde ist Robert C. Post, der 1989 nach den „social foundations“ fragt, damit aber auch nicht die gesellschaftlichen, sondern eigentlich ausschließlich die gemeinschaftlichen meint.[1355] Das wird gerade auch an den Stellen deutlich, wo er nicht – wie sonst über die ganze Arbeit verteilt – Simmel oder Goffman zitiert, sondern Merton oder Parsons:[1356] Selbst dort, wo strukturfunktionalistische Theorie referenziert wird, geschieht das nur aus individualistischer oder gemeinschaftlicher Perspektive. Jed Rubenfeld hingegen beschäftigt sich im gleichen Jahr mit dem verfassungsrechtlichen Recht auf *privacy* in Abgrenzung zu den *privacy*-Erwartungen nach dem Fourth Amendment und dem *privacy*-Schutz aus dem „tort law“.[1357] Rubenfeld lehnt dabei die „personhood“-Theorie ab, wonach Menschen sich durch die Selbstbestimmung zugleich selbst in ihrer Identität definieren würden, und fordert stattdessen, dass die Selbstbestimmung verstanden werde als Abwehrrecht gegen das „being forced into an identity“ und somit als „anti-totalitär“.[1358] Daraus folgert er dann, dass jeweils gefragt werden müsse, was durch eine staatliche Handlung oder ein Gesetz „produziert“ werde: „Mütter“ durch Abtreibungsverbote, „Rassenreinheit“ durch Rassentrennungsgesetze und „a »standardization« of lives that it considered unacceptable“ durch Wohnbeschränkungsregelungen.[1359]

Von dieser Fixierung auf das Private und das Öffentliche als Referenzpunkte kann sich auch Simitis nicht trennen, wenn er den Stand der bundesdeutschen Debatte einem amerikanischen Publikum nahebringt, während er gleichwohl – wenn auch nur in einer Fußnote – *privacy* schlicht mit dem allgemeinen Persönlichkeitsrecht gleichsetzt und zugleich in dem gesamten Text ausschließlich über *information privacy* spricht.[1360] Dafür weist er das Problem jedoch explizit als

[1351] Siehe Allen (1988, S. 3, 11 ff., 15). Allen will damit explizit mehr als nur *informational privacy* abdecken (S. 8), nicht jedoch *decisional privacy* (S. 32). Allens Definition von *privacy* ist die gleiche wie die von Ruth Gavison, siehe Gavison (1980).

[1352] Siehe Allen (1988, S. 54 ff.). Das Problem ist, dass sie die Relativität des *privacy*-Begriffs offensichtlich nicht wirklich versteht, also die Unterscheidung danach, gegen welche soziale Akteurin oder gegen welchen anderen Begriff hier jeweils „privat“ verwendet wird, siehe dazu S. 55, Endnote 4. Zu ersterem siehe schon Steinmüller et al. (1971, S. 51), zu letzterem ausführlich Geuss (2013).

[1353] Siehe Allen (1988, S. 123 ff.).

[1354] Später wird sie die so verstandene „privacy“ mit „accountability“ als Gegenkonzept kontern, siehe Allen (2003).

[1355] Siehe insbesondere die Ausführungen am Ende der Einleitung, Post (1989, S. 959). Ganz überraschend ist das natürlich nicht, schließlich geht es in seiner Arbeit um das Recht der unerlaubten Handlungen – „tort law“ –, das historisch einfach schon sehr auf interpersonale Beziehungen ausgerichtet ist.

[1356] Siehe Post (1989, S. 969, 977).

[1357] Siehe Rubenfeld (1989).

[1358] Siehe Rubenfeld (1989, S. 782, 796).

[1359] Siehe Rubenfeld (1989, S. 783, 788, 791 und 792). Die auf dieser Konzeption aufbauenen Ausführungen in der Analyse eines Gesetzes, das homosexuellen Sex verbietet (S. 799 ff.), erscheinen jedoch arg konstruiert und überzeugen nicht, obwohl das Verständnis von *privacy* als Mittel zur Verhinderung von Fremdzuweisung von Identität durchaus als für die Datenschutzdebatte anschlussfähig scheint, siehe dazu die Herrmann Göring zugeschriebene Aussage: „Wer Jude ist, bestimme ich.“

[1360] Siehe Simitis (1987, S. 708, Fn. 7). Korrekter wäre allerdings zu schreiben, Simitis gebe den Stand der Debatte nur insoweit wieder, wie er dafür eine seiner Arbeiten als Quellen anführen oder die Quellen ganz weglassen könne.

nicht-individuelles aus, sondern als eines, dass alle betrifft.[1361] Er stellt fest, dass „surveillance“ ihren Ausnahmecharakter verloren habe und mehr und mehr zur Routine geworden sei.[1362] Und drittens weist Simitis darauf hin, dass personenbezogene Informationen zunehmend genutzt würden, um Verhaltensnormen durchzusetzen.[1363] Darüber hinaus wiederholt er seine im Jahr zuvor geäußerten Befürchtungen der Generierung von Personengruppen in der und durch die Datenverarbeitung und der anschließend erfolgenden Beurteilung der Betroffenen anhand der Zugehörigkeit zu einer der Gruppen[1364] mit der Folge der Institutionalisierung von Kontrolle.

Die Verbindung zu Foucault, die Simitis in seinem Artikel herstellt, ist nicht zufällig, denn etwa zur gleichen Zeit betritt eine neue Theorieschule die Bühne des Diskurses: die später so genannten Surveillance Studies, die im wesentlichen auf Vorarbeiten von Michel Foucault aufsetzen. Der Begriff „surveillance“ bezeichnet dabei im Grunde nichts anderes als „Informationsverarbeitung über Menschen und Dinge“ im weitesten Sinne, wenn auch manchmal gedacht als „mit dem Ziel von Kontrolle“ und manchmal nicht, manchmal eingeschränkt auf „systematische“ *surveillance* und manchmal nicht, jedoch immer unter Ausschluss von „Entscheidung“.[1365] Die Gesellschaft, die durch solche Überwachungspraktiken geprägt werde und von einer Bürokratisierung der sozialen Kontrolle geprägt sei, wird dementsprechend als „surveillance society“ bezeichnet.[1366] Das Verhältnis der Surveillance Studies zur *privacy*-Forschung ist extrem ambivalent: Gerade in den ersten Jahren wird stark auf –jedenfalls Teilen – der vorhergehenden *privacy*-Debatte aufgebaut und immer wieder *privacy* als das zentrale Schutzgut herausgestellt.[1367] Später wird darüber jedoch ausgiebig gestritten[1368] – nicht wirklich überraschend, denn die Surveillance Studies haben nicht *privacy* als zentralen Bezugspunkt, sondern die als *surveillance* bezeichneten Informationsverarbeitungsprozesse, und diese können sehr wohl – etwa bei der *surveillance* von Dingen – ganz ohne jede Verbindung zu *privacy* problematisiert werden.

Oscar H. Gandy liefert dazu Anfang der 90er Jahre eine der ersten beiden umfassenden – und in den Surveillance Studies als grundlegend angesehen werdenden – Arbeiten über das „panop-

[1361] Siehe Simitis (1987, S. 709 f.), wobei Simitis' Formulierung „conflicts affecting everyone“ durchaus mehrdeutig ist, weil sie im Englischen auf Gruppen von Individuen wie auf Gesellschaften passt – im ersten Fall wären sie immer noch individuelle Probleme, nur eben von vielen Individuen. Nur im zweiten Fall wären sie explizit als gesellschaftliche Probleme markiert.

[1362] Siehe Simitis (1987, S. 710), ohne jedoch auszuweisen, warum er hier den Begriff der „surveillance“ nutzt und nicht den des „information processing“. Die Ausführungen auf S. 729 und in den Fußnoten 97 und 98 legen eine Übernahme des Begriffs von Michel Foucault via Gary Marx und Nancy Reichman nahe, siehe Marx und Reichman (1984).

[1363] Siehe Simitis (1987, S. 710).

[1364] Siehe Simitis (1987, S. 719, 728) und Simitis (1986, S. 29). Ein Teil der Surveillance Studies wird das später übernehmen, und mehr als zehn Jahre nach Simitis wird Anton Vedder das gleiche Problem neuentdecken, es als „deindividualization of the person“ bezeichnen und mit dem Term „categorical privacy“ adressieren, siehe Vedder (1999).

[1365] Siehe dazu die Übersicht bei Marx (2015, S. 734 ff.).

[1366] Siehe zum Beginn dieser Debatte Marx (1985), der wohl auch den Begriff der „surveillance society“ prägt, und nachfolgend Flaherty (1988) und Flaherty (1989b) sowie Gandy (1989). Einer der Gegenbegriffe für im wesentlichen das gleiche Konzept, der sich jedoch nicht durchsetzen konnte, ist der der „dossier society“, siehe Laudon (1986b).

[1367] Siehe etwa die umfassenden Ausführungen dazu bei Gandy (1993, S. 137 ff.), dagegen allerdings Lyon (1994, S. 170 ff. und 179 ff.), dann jedoch wieder dafür Lyon und Zureik (1996).

[1368] Siehe etwa Stalder (2002a) für eine scharfe Trennung zwischen *privacy* und *surveillance* oder die aufkommende Auseinandersetzung, nachdem Colin Bennett *privacy* als Konzept und Regime für die Surveillance Studies verteidigte, Bennett (2011a): die zustimmende Antwort von Regan (2011) und die ablehnenden Antworten von Gilliom (2011) und Stalder (2011) sowie die Reaktion darauf von Bennett (2011b). Und Coll (2014) sieht *privacy* sogar als eine Verbündete von *surveillance*, weil und soweit sie vermittels des Selbstbestimmungsprinzips übermäßig individualistisch konzeptionalisiert sei.

tic sort", „the all-seeing eye of the difference machine that guides the global capitalist system", und meint damit „a kind of high-tech cybernetic triage through which individuals and groups of people are being sorted according to their presumed economic or political value."[1369] Gandy versteht dabei das „panoptic sort" als eine Ausdehnung technischer Rationalität in den sozialen Bereich durch organisierte soziale Akteurinnen – „bureaucratic organizations" – innerhalb vermachteter sozialer Beziehungen.[1370] „Panoptic sort" bestehe aus drei miteinander verbundenen Prozessen: „identification, classification, and assessment".[1371] Es gehe erstens um die Identifikation der zu kontrollierenden Betroffenen, die zweitens auf der Basis der sie beschreibenden Informationen in Klassen eingeteilt würden, wobei die Klasseneinteilung selbst wiederum Ergebnis einer Bewertung von Normalität und Unterschied sei. In solchen Prozessen würden Vorurteile institutionalisiert und zugleich Informationen dekontextualisiert, wobei die Fehlrepräsentation des Kontexts selbst wieder das Ergebnis von Vorurteilen sei. In den vermachteten Strukturen sei die Macht, die Betroffenen gegenüber Organisationen erwüchse, wenn sie diesen Informationen vorenthalten würden, unerheblich im Vergleich zu der Macht, die Organisationen hätten, indem sie Güter oder Dienstleistungen zurückhalten könnten, wenn die Betroffenen Informationen über sich nicht preisgeben würden. Die technischen Systeme – denn „panoptic sort" bezeichnet nur die technischen, nicht aber die techno-sozialen Systeme – seien geprägt von einer instrumentellen Rationalität, und sie würden gerade deshalb so gestaltet, um den Interessen ihrer Betreiberinnen zu dienen.[1372] Im Gesamtblick präsentiert Gandy mit seiner Arbeit eine fast deckungsgleiche Analyse zu den Datenschutzanalysen der 70er Jahre,[1373] wenn auch durchaus mit Unterschieden, nicht nur bei den zugrunde gelegten Theorien. So hält Gandy etwa die Sensitivität von Informationen für einen geeigneten Maßstab für eine Regulierung.[1374]

Die andere für die Surveillance Studies grundlegende Arbeit entstammt der Feder David Lyons.[1375] Auch für diese Arbeit gilt das vorstehende – die Überschneidungen mit den Arbeiten zum Datenschutz aus den 70ern sind unübersehbar.[1376] Für Lyon ist *surveillance* „a shorthand term to cover the many, and expanding, range of contexts within which personal data is collected by employment, commercial and administrative agencies, as well as in policing and security" und besitze zwei Gesichter: „The processes that may seem to constrain us stimultaneously [sic!] ena-

[1369] Siehe Gandy (1993, S. 1 f.). An anderer Stelle bezeichnet er es als „the complex technology that involves the collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers and is used to coordinate and control their access to the goods and services that define life in the modern capitalist economy", als „difference machine that sorts individuals into categories and classes on the basis of routine measurements" sowie als „system of power", siehe S. 15.

[1370] Siehe Gandy (1993, S. 2 f.). Er baue dabei auf den Theorien von Marx, Ellul, Weber, Foucault und Giddens auf, so Gandy, siehe S. 3 ff.

[1371] Siehe dazu und zum folgenden Gandy (1993, S. 15 ff.).

[1372] Siehe Gandy (1993, S. 80 und 95).

[1373] Das ist schon deshalb nicht überraschend, weil sich Gandy etwa auf Simitis stützt, siehe etwa S. 201, auch wenn er offensichtlich nicht weiß oder ignoriert, dass es sich dabei nicht allein um Simitis' „insights" handelt, sondern um das Ergebnis einer langen und komplexen Auseinandersetzung um die Begründung des Datenschutzes, die am Ende gerade zu dem Volkszählungsurteil geführt hatte, aus dem die Aussage entnommen wurde – bei Simitis korrekt zitiert, siehe Simitis (1987, S. 734), bei Gandy mit der falschen Seitenzahl angegeben („p. 735"), siehe Fn. 87.

[1374] Siehe Gandy (1993, S. 198 ff.).

[1375] Siehe Lyon (1994), der sich wie Gandy auf Theorien von Marx, Weber und Foucault stützt.

[1376] Der Grund, warum dies von den beteiligten nicht wahrgenommen wurde und wird, könnte in einer *déformation professionelle* liegen: Soziologinnen nehmen nur soziologische Vorarbeiten als Vorarbeiten wahr. Siehe dazu Lyon (1994, S. 6), wo der Autor auf Rule (1973) als einzige sozialwissenschaftliche Vorarbeit, trotz der Tatsache, dass Alan Westin nicht nur Jurist, sondern auch Politikwissenschaftler war, und Paul Müller sogar Soziologe – und mindestens einmal in Englisch publizierte, siehe Müller und Kuhlmann (1972).

ble us to participate in society.“[1377] Es handele sich dabei um eine Folge der für bürokratische Organisationen bestehenden Notwendigkeit, einen Überblick über eine zunehmend komplexer werdende Gesellschaft mit einer großen Vielfalt an Gruppen zu behalten.[1378] Eine Folge davon sei ein verändertes Verhältnis zwischen Organisationen und ihrem Klientel, denn dieses Verhältnis werde nun „mediated by the data collected“ und Entscheidungen über Betroffene seien darum „closely tied to available information about those subjects.“[1379] Von einer Lösung durch Recht hält Gandy nichts und fordert stattdessen „[s]ocial, cultural and political approaches“, wobei sein Wissen um das Recht und dessen historische Konstruktion allerdings, wie seine Ausführungen zeigen, nicht sehr groß ist.[1380] Während dieses fehlende Verständnis seine Ablehnung von Recht als geeigneter Lösung erklären könnte, ist seine Unkenntnis der *information privacy*-Konstruktion und ihrer Geschichte – so schreibt er Westins *privacy* als *claim to control the information flow* einfach dem von der britischen Regierung eingesetzten *Lindop Committee* und dem Jahr 1978 zu[1381] – wahrscheinlich der Grund für seine Ablehnung jeder Anknüpfung an die *privacy*-Debatte.[1382] Vor diesem Hintergrund überrascht sein Lösungsvorschlag – oder auch nicht. Auf der einen Seite „controlling the circulation of personal information is a question of the appropriateness of disclosure within differing contexts“, denn „access to particular information is systematically related in the appropriate way to the network of social relationships in which that person stands to others by virtue of their places in the role structure“,[1383] auf der anderen Seite „personhood centred on self-communication“ mit „human dignity and human freedom“ mit Referenz zu Habermas' Theorie des kommunikativen Handelns mit seinen idealen Sprechsituationen[1384] und das Ganze zusammengefasst unter der Trinität von „participation, personhood and purposes“, denn: „From »participation« derive some alternatives to the exclusionary power of much surveillance, from »personhood« some criteria by which to judge the data-image, and from »purposes« an antidote to the self-augmenting development of surveillance technologies.“[1385]

Beide Werke lesen sich, und das überrascht durchaus ein wenig, über weite Strecken wie eine überarbeitete Version von Vance Packards „The Naked Society“[1386] und zugleich – jedenfalls aus Sicht einer Technikwissenschaft – oberflächlicher, als das zu dieser Zeit verfügbare Wissen über Informationstechnik und moderne Informationsverarbeitung in Organisationen hergeben würde.

„Surveillance“ ist aber nicht der einzige Begriff, der sowohl die Realität moderner Informationsverarbeitung in den Vordergrund stellt – und nicht das (echte oder vermeintliche) Schutzgut –, und dem es zugleich gelingt, eine Gruppe Gleichgesinnter um sich zu scharen. Gleiches gilt für Roger Clarkes Begriff der „Dataveillance“, bei dem es sich um eine Zusammenziehung von „data surveillance“ handelt, und mit dem Clarke „the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons“

[1377] Siehe Lyon (1994, S. ix).
[1378] Siehe Lyon (1994, S. 4).
[1379] Siehe Lyon (1994, S. 84).
[1380] Siehe Lyon (1994, S. 171 f.).
[1381] Siehe Lyon (1994, S. 187). Das wirkliche Problem, so zitiert Lyon Geoffrey Brown, sei „the possibility of the wrong bits of information getting into the wrong hands, or getting there by the wrong means or through the wrong channels“, ebd. Gut zu wissen! Und warum ist jetzt noch mal nicht die gleiche Informationsflusskontrolle, die alle anderen auch fordern?
[1382] So scheinen jedenfalls seine Ausführungen zu verstehen zu sein, siehe Lyon (1994, S. 189).
[1383] Siehe Lyon (1994, S. 194).
[1384] Siehe Lyon (1994, S. 196 ff.).
[1385] Siehe Lyon (1994, S. 214).
[1386] Siehe Packard (1964).

bezeichnen will.[1387] Darauf aufbauend analysiert er dann etwa das Problem des Profiling und kreiert – ob in Unkenntnis von oder Ignoranz gegenüber der vorhergehenden Diskussionen zu Datenschatten[1388] – das Konzept der „digital persona“ im Sinne eines Personenmodells,[1389] um sich später dem Thema „Privacy Impact Assessments“ zuzuwenden – einem Konzept, das Clarke zumindest mitentwickelt hat.[1390]

Obwohl schon vorher immer wieder rechts- und politikvergleichende Arbeiten publiziert worden waren,[1391] gab es gerade zwischen Mitte der 80er und Mitte der 90er Jahre einen wahren Boom solcher Arbeiten.

In einer dreiteiligen Arbeit analysiert Michael Rogers Rubin im ersten Teil die durch moderne Informationsverarbeitungspraktiken erzeugten *privacy*-Probleme, im zweiten Teil die verschiedenen Antworten, die darauf in verschiedenen Ländern gegeben wurden, sowie deren Geltungsbereiche und Durchsetzungsansätze, und im dritten Teil die Regulierung in den USA im Detail.[1392] Er ordnet die Probleme, die er als „abusive practices“ bezeichnet, in drei Bereiche – „areas of attack“ – ein. Mit „abusive collection practices“ will er unfaire Erhebungsmethoden und die Erhebung von für die angegebenen Zwecke ungeeigneten Informationen adressieren, während er mit „abusive dissemination practices“ eigentlich Verarbeitungspraktiken wie „computer matching“ einerseits und Nutzungen für andere als die angegebenen Zwecke andererseits problematisieren will und mit „abusive management practices“ adressiert er schließlich die Nichtinformation der Betroffenen, die Nichtgewährung von Betroffenenrechten auf Einsicht und Korrektur sowie den Widerwillen zur Korrektur weitergegebener falscher Informationen auf Seiten der Organisation.[1393] Anhand dieser Dreiteilung untersucht er dann die Regelungsansätze in verschiedenen Ländern – Canada, Dänemark, Deutschland, Frankreich, Großbritannien, Luxemburg, Norwegen, Österreich, Schweden – sowie der OECD und des Europarats[1394] und stellt fest, dass sie einander stark ähneln, wobei er allerdings nur prüft, ob die von ihm im ersten Teil identifizierten Probleme adressiert werden.[1395] Während die meisten Länder umfassende Datenschutzgesetze erlassen haben, existieren in de USA ausschließlich sektor- und ebenenspezifische *privacy*-Gesetze mit im Ergebnis großen Schutzlücken sowohl im Bereich der öffentlichen wie der nicht-öffentlichen Informationsverarbeitung.[1396]

Zu einem ähnlichen Ergebnis kommt David H. Flaherty in seiner viel tiefer gehenden und stark auf Interviews mit verschiedenen Stakeholdern basierenden Untersuchung der datenschutzrechtlichen Regelungen in Canada, Deutschland, Frankreich, Großbritannien und den USA sowie der

[1387] Siehe Clarke (1988, S. 499).
[1388] Siehe etwa Westin (1967, S. 163 ff.) und Anér (1972).
[1389] Siehe Clarke (1993) und Clarke (1994).
[1390] Siehe Clarke (1999) und Clarke (2009). Siehe aber auch den schon Ende der 1980er bei Flaherty (1989a, S. 405) zu findenden Verweis auf „privacy impact statements“.
[1391] Siehe etwa Strömholm (1967), Kamlah (1969) und Kamlah (1971a), Hondius (1975) sowie Rule et al. (1980).
[1392] Siehe Rubin (1987), Rubin (1988) und Rubin (1989).
[1393] Siehe Rubin (1987).
[1394] Rubin ist dabei der erste in einer langen Reihe von Autorinnen, die – ohne tatsächlich dafür Belege vorzubringen – behaupten, der amerikanische Ansatz eines „Code of Fair Information Practice“, siehe U.S. Department of Health, Education, and Welfare (1973), habe einen größeren Einfluss auf die nationalen Regelungen gehabt als die jeweiligen Gutachten, die in den anderen Ländern veröffentlicht wurden, siehe Steinmüller et al. (1971), Task Force on Privacy and Computers (1972), Offentlighets- och sekretesslagstiftningskommittén (1972) und Younger (1972), *obwohl sie alle vorher erschienen sind*, siehe Rubin (1988, S. 89 f.). Alternativ wird auch gerne behauptet, alle nationalen Gesetzgeber hätten von der OECD „abgeschrieben“, siehe etwa Birnhack (2013).
[1395] Siehe Rubin (1988).
[1396] Siehe Rubin (1989).

Rolle der Aufsichtsbehörden in den betreffenden Jurisdiktionen.[1397] Flaherty will untersuchen, wie effektiv der Schutz der *privacy* durch Gesetze und Aufsichtsorgane gegen „the emergence and installation of surveillance societies“ sichergestellt wird.[1398] Wie die meisten Autorinnen hat auch Flaherty einen vordefinierten Begriff davon, was *privacy* sei – Ruth Gavisons „limitation of others' access to an individual“ –, und dieser ist, jedenfalls auf der Ebene der zugrunde gelegten Theorie, beschränkt auf interpersonale Beziehungen und auf der Ebene der Problembeschreibung zugleich ausgerichtet auf „the growing power of large public and private institutions in relation to the individual citizen.“[1399] Im Ergebnis stellt er zwar durchaus nationale Besonderheiten fest, gerade auch hinsichtlich verschiedener Verfassungstraditionen, aber im Großen und Ganzen seien sowohl die adressierten Probleme wie die Lösungsansätze vergleichbar, wobei er zugleich den europäischen Datenschutzgesetzen eine „hidden agenda“ zuschreibt, nämlich die Verhinderung einer Wiederkehr des Nazismus mit seinem Ziel der Bevölkerungskontrolle.[1400] Darüber hinaus trennt er zwischen *privacy* und Datenschutz, wobei er nur letzteres in *allen* Gesetzen, auch den kanadischen und US-amerikanischen Privacy Acts, umgesetzt sieht, und verweist für die Definition von Datenschutz auf die Definition des Europarats, wonach Datenschutz „the legal protection of individuals with regard to automatic processing of personal information relating to them“ sei.[1401] Hingegen hält er *privacy* und *privacy interests* für viel breiter und – ohne Begründung – für in allen westlichen Ländern in ihrem Kern gleich, ohne sie allerdings angeben zu können; stattdessen verweist er auf „Freiheit“ und „Gleichheit“, für die das auch nicht angeben werden könne, und darauf, dass es um das gehe „what each of us thinks and feels about his or her own interests in a value like privacy“.[1402] Alles, was Flaherty daraus aber zieht, sind dann wieder nur abstrakte Prinzipien „for the control of surveillance“, die er als „Data Protection Principles and Practices“ bezeichnet und die weitgehend den „Fair Information Practice Principles“ folgen.[1403]

[1397] Siehe Flaherty (1989a), zu letzterem siehe auch umfassend Flaherty (1986). Leider legt Flaherty nicht offen, mit wem er alles gesprochen hat – an einer Stelle allerdings dankt er Herbert Burkert, der ihm erklärt habe, das Bundesverfassungsgericht habe im Volkszählungsurteil eine Definition von *privacy* abgegeben, die nahe an der von Westin sei, siehe S. 34, Endnote 18 (S. 414). Die Ausführungen zum Gesetzgebungsverfahren in der BRD sind jedenfalls ziemlich oberflächlich und stark von den wenigen – und ausschließlich englischsprachigen – Texten geprägt, die Flaherty gelesen und zitiert hat – und der Auswahl seiner Interviewpartnerinnen, zu denen neben Burkert offensichtlich vor allem Datenschutzbeauftragte wie Simitis zählten, siehe S. 47, Endnote 25 (S. 415). Auch die Ausführungen zu Bull und Reinhold Baumann, Bulls Nachfolger als Bundesdatenschutzbeauftragter, legen ein Interview oder Interviews mit diesen nahe. Flaherty schreibt daher viele Entwicklungen seinen Gesprächpartnerinnen zu, die sie historisch nicht – oder zumindest nicht in diesem Umfang – beeinflusst haben, wie Simitis' vermeintliche Rolle im Volkszählungsverfahren vor dem BVerfG, siehe S. 80. Das gleiche Problem zeigt sich in der Regulierungsanalyse von Bennett (1991, S. 66, Note 7 (S. 67)), der fälschlich behauptet, das Hessische Datenschutzgesetz habe einen großen Einfluss auf die nachfolgende Verregelung gehabt.

[1398] Siehe Flaherty (1989a, S. 13).

[1399] Siehe Flaherty (1989a, S. 7 ff.) mit Verweis auf Arnold Simmel und David Burnham, auf einen von der Öffentlichkeit abgetrennten „private realm“ als Schutzbereich sowie mit dem Glauben an die Sensitivität als Eigenschaft von Informationen. Siehe auch S. 398 für Flahertys Sicht auf Datenschutz als „reinforcement of the traditional rights of individuals among themselves and with respect to groups“.

[1400] Siehe Flaherty (1989a, S. 317 ff.).

[1401] Siehe Flaherty (1989a, S. 377 und Endnote 13 (S. 462).).

[1402] Siehe Flaherty (1989a, S. 378 f.).

[1403] Siehe Flaherty (1989a, S. 380).

Auch Colin J. Bennett kommt in seinen Untersuchungen zu grundsätzlich vergleichbaren, wenn auch differenzierteren Ergebnissen.[1404] So untersucht er die Konvergenz von vier nationalen Regelungen – Deutschland, Großbritannien, Schweden, USA –, ob sie das Produkt eines technischen Imperativs, von Emulation, von Harmonisierung oder durch direkte Einflussnahme von Akteurinnen eines Landes auf die Gesetzgebung eines anderen sind, und kommt zu dem Ergebnis, dass die Entstehung einer „transnational policy community", die gemeinsame Basis in der liberal-demokratischen Ideologie, gleiche oder sehr ähnliche Vorstellungen zu Computern, *privacy*- und Persönlichkeitsrechten sowie effektiven Regelungsansätzen und der durch die OECD und den Europarat geschaffenen institutionellen Rahmen für eine internationale Debatte zur Regulierung des *privacy*-Problems nur zusammen eine sinnvolle Erklärung liefern könnten.[1405] Nachfolgend versucht Bennett, die Regelungsansätze Canadas, Deutschlands, Großbritanniens, Schwedens und der USA auf drei einschlägige Regulierungstheorien – „a technology control theory, a civil rights theory, and an institutional accountability theory" – zu mappen, wobei das Datenschutzrecht in Großbritannien und Schweden am ehesten der ersten, das US-amerikanische Recht im wesentlichen der zweiten und das deutsche und das kanadische Recht am ehesten der dritten Theorie entsprechen würde.[1406] Seine Schlussfolgerung, in der er vor dem Hintergrund der technischen und gesellschaftlichen Entwicklungen fordert, „a more complete understanding of the relationship between bureaucratic organization and technology is necessary — the information technology practices of organizations, in other word" zu entwickeln,[1407] zeigt allerdings, dass er die umfangreichen Vorarbeiten in dieser Richtung durch die deutsche Datenschutzdebatte der 1970er nicht kennt. Grundsätzlich sei jedenfalls die Konvergenz auf der Ebene der Prinzipien größer als auf der Ebene der spezifischen Regelungsinstrumente.[1408] Abschließend versucht er, aus drei Perspektiven eine zusammenfassende Einschätzung zum Datenschutzrecht und seiner Zukunft abzugeben, wobei er offensichtlich Datenschutz und Datenschutzrecht gleichsetzt: Aus humanistischer Sicht sei Datenschutz „a symbolic attempt to protect a lost value" gegen den Drang nach Effizienz und Kontrolle durch moderne, bürokratische Organisationen, aus politischer Sicht sei *privacy* nur ein Interesse unter vielen im politischen Prozess mit sehr gemischten Ergebnissen – Erfolgen wie Niederlagen – und in instrumenteller Hinsicht könne die Integration von „fair information practice" in Organisationen als Teil einer Entwicklung zu einer umfassenderen Informationspolitik verstanden werden.[1409] Jedenfalls, so statuiert Bennett, „the roots of data protection are individualistic" und würden zum Schutz von „a *preindustrial* value" in einem „*postindustrial* state" dienen.[1410]

[1404] Bennett hat Anfang der 1990er Jahre eine sehr umfassende Analyse veröffentlicht, siehe Bennett (1992), der mehrere spezifischere Einzelstudien seit Ende der 1980er Jahre vorausgingen, unter anderem Bennett (1988) und Bennett (1991).

[1405] Siehe Bennett (1988). Die Ausführungen sind historisch allerdings nur teilweise korrekt und oft verkürzt, und jedenfalls für die Bundesrepublik werden Simitis' Rolle und die Rolle des Hessischen Datenschutzgesetzes exzessiv überbewertet, siehe S. 428.

[1406] Siehe Bennett (1991).

[1407] Siehe Bennett (1991, S. 64).

[1408] Siehe Bennett (1992). Allerdings ist seine Analyse jedenfalls insofern mit Vorsicht zu genießen, als dass sie unter anderem auf der Einschätzung basiert, die Datenschutzgesetze würden auf der Annahme basieren, Datenverarbeitung fände in einer „single, powerful, but bounded »databank«" statt, siehe S. 246.

[1409] Siehe Bennett (1992, S. 251 ff.). Siehe zu letzterem schon Podlech (1973b), Steinmüller (1976c) und Fiedler (1981), die Bennett aber offensichtlich nicht kennt.

[1410] Siehe Bennett (1992, S. 253), Hervorhebungen im Original.

Während Priscilla M. Regan Mitte der 1980er auch noch zu dieser rechts- und politikvergleichenden Debatte beitrug,[1411] wandte sie sich aber Ende der 1980er der Analyse der amerikanischen *privacy*-Debatte und -Gesetzgebung zu.[1412] So analysiert sie etwa den Privacy Act of 1974 und die ihm zugrunde liegenden Fair Information Practice Principles vor dem Hintergrund neuerer technischer Entwicklungen – der zahlenmäßigen Zunahme der gespeicherten Daten, der qualitativen Änderungen in den Informationsverarbeitungsprozessen durch die Computerisierung, der Einführung von PCs, neuen Suchverfahren („types of searches“) wie „matching“ und „profiling“ sowie der zunehmenden Vernetzung von Systemen – und kommt zum Schluss, dass die FIPPs in weiten Bereichen der amerikanischen Verwaltung, die unter den Privacy Act fallen, nicht befolgt würden *und daher veraltet seien.*[1413] Auch ihr Buch, „Legislating Privacy“, ist von dieser etwas abstrusen Sicht auf die Funktionsweise und die Grenzen von Recht geprägt, darüber hinaus aber auch von einer – jedenfalls teilweise – willkürlichen Unterteilung von *privacy* in „information privacy“, „communication privacy“ und„psychological privacy“, gefolgt von weiteren „privacy issues“ wie „medical privacy“.[1414] Für alle drei Bereiche konstatiert Regan:

> „a similar pattern regarding the dynamics of the congressional policy debate emerges — initial definition of the policy problem as one of privacy invaded by new technology; opposition by those who benefited from use of the new technology and from redefinition of the problem; continued pressure by a small but vigilant privacy community that relied for support on the members and staff of key congressional committees; and, after years, passage of weakened legislation.“[1415]

In allen drei Fällen seien die *privacy*-Interessen als individuelle, nicht als gesellschaftliche Interessen markiert worden, denen die Gegeninteressen durchgängig als gesellschaftliche Interessen gegenübergestellt wurden.[1416] Regan ist die erste, die in der englischsprachigen Debatte die Tatsache explizit aufgreift, dass die meisten Debattenbeiträge, insbesondere die philosophischen, sich nicht auf gesellschaftliche, sondern auf zwischenmenschliche Verhältnisse beziehen, und das als Problem sieht.[1417] Allerdings sind ihre Versuche, *privacy* als „common value“, „public value“ und „collective value“ zu verkaufen,[1418] nicht sehr überzeugend, unter anderem weil auch sie sich nicht von der konzeptionellen Bindung an *privacy* als einen von der Öffentlichkeit getrennten Zustand und zugleich als Geheimnis trennen kann.

Diesen Ansätzen diametral gegenüber steht Paul M. Schwartz, der Ende der 1980er Jahre vorschlägt, das Recht auf informationelle Selbstbestimmung in das amerikanische Verfassungsrecht zu übernehmen, und dabei nicht nur wesentliche Argumentationsfiguren aus der deutschen

[1411] Siehe etwa Regan (1984) zur Frage der Durchsetzung von Interessen in verschiedenen Phasen der Politikformulierung und Gesetzgebung am Beispiel von Datenschutzregelungen in Großbritannien und den USA.

[1412] Siehe Regan (1988) und vor allem ihr umfassendes Werk, „Legislating Privacy“, Regan (1995).

[1413] Siehe Regan (1988). Siehe aber auch Matleys Einschätzung, dass der Privacy Act of 1974 schon durch die ihm eingeschriebenen Beschränkungen und die unzähligen Ausnahmen keinen Schutz habe bieten können, Matley (1985, S. 221), und Grays' Ausführungen weisen darauf hin, dass einer der Gründe für das Scheitern in der übermäßigen Konkretheit von Regelungen liegen könnte, die daher leicht zu umgehen seien, siehe Gray (1989).

[1414] Siehe Regan (1995, S. xv und 7 ff.). Mit „psychological privacy“ adressiert Regan das bei Westin unter „psychological surveillance“ subsumierte Erheben von Informationen mittels Lügendetektoren u. ä., siehe Westin (1966a, S. 1004). Für eine Analyse der „communication privacy“, die auch die Crypto Wars der 1990er Jahre mit einschließt, siehe Diffie und Landau (1998).

[1415] Regan (1995, S. 22). Siehe auch S. 174 ff. und den Hinweis auf S. 178, dass in der politischen Debatte *privacy* jeweils durch seine Substitute ersetzt wurde, etwa *information privacy* durch *fair information principles.*

[1416] Siehe Regan (1995, S. 22 f.).

[1417] Siehe Regan (1995, S. 25 ff.).

[1418] Siehe Regan (1995, S. 212 und 220 ff.).

Datenschutzdebatte übernimmt, sondern auch behauptet, das deutsche Datenschutzrecht zeige, dass ein solches Recht nicht auf der Basis einer „legal idea of privacy“ entwickelt werden könne. Stattdessen müsse die Regulierung auf einer Analyse der „dangers of specific data processing constellations in which individual information is employed“ aufsetzen.[1419] In die gleiche Richtung argumentiert er drei Jahre später, indem er den amerikanischen Ansatz, die öffentliche Verwaltung, die einem „*data processing model* of administrative control“ folge und die er daher als „processors of information“ bezeichnet, und deren Informationsverarbeitung unter Kontrolle zu bringen, als gescheitert erklärt.[1420] Schwartz zeigt, dass *privacy* als Paradigma für eine rechtliche Regulierung ausgedient hat – erstens wegen der konzeptionellen Bezugnahme auf einen „private space“ und zweitens wegen der Beschränkung auf „intimate or familial activities or information about such activities“ – und stellt dem zwei „neue“ Prinzipien als Ersatz gegenüber: „bureaucratic justice“ und „human autonomy“.[1421] Diese Prinzipien sollen dann in einem explizit am Modell des deutschen Datenschutzrechts ausgerichteten Datenschutzgesetz umgesetzt werden, mit dem die Transparenz der bürokratischen Systeme erzwungen und ein unabhängiges Aufsichtsorgan institutionalisiert werden würden.[1422]

2.4.4 Recht als Technikgestalter und die relative Betriebsblindheit der Informatik

Auch die – im weitesten Sinne – informatische Diskussion war zwischen Mitte der 80er und Mitte der 90er Jahre von einer Zweiteilung geprägt.[1423] Auf der einen Seite standen die Arbeiten, die sich mit der Frage der *privacy-* und datenschutzfreundlichen bzw. der datenschutzrechtskonformen Gestaltung von technischen und soziotechnischen Systemen beschäftigten, auf der anderen Seite fokussierte die vor allem aus der Kerninformatik gespeiste Debatte auf Anonymität und Anonymisierung als Schutzmechanismen. Die Gestaltungsdebatte bleibt dabei bis zur Freigabe des Internets für kommerzielle Zwecke Mitte der 90er Jahre und der Einführung des *Health Insurance Portability and Accountability Act* (HIPAA) 1996 mit seiner „Privacy Rule“ – von Ausnahmen aus dem Bereich der *Computer-supported cooperative work* abgesehen – vorwiegend auf die Bundesrepublik beschränkt.

Beide Stränge der Diskussion trafen aber auch zusammen, an manchen Stellen unter expliziter Einbeziehung nicht-informatischer Sichtweisen. Ein Beispiel für ein solches Zusammentreffen ist die erste GI-Fachtagung des Arbeitskreises „Datenschutz und Datensicherung“ des Präsidiums der GI zum Thema „Datenschutz und Datensicherung im Wandel der Informationstechnologien“ im Oktober 1985 unter Teilnahme von Informatikerinnen und Juristinnen, Wissenschaftlerinnen

[1419] Siehe Schwartz (1989, S. 676 f.), allerdings auf der Basis von Theorien über interpersonale Beziehungen, siehe S. 683, vor allem Fn. 42. Schwartz war in den 1980er Jahren Post-Doc bei Spiros Simitis, wie Herbert Burkert in einem persönlichen Gespräch am Rande eines Steinmüller-Kolloquiums bemerkte.

[1420] Siehe Schwartz (1992, S. 1325), Hervorhebung im Original. Die theoretische Grundlage für seine Analyse ist Benigers „control revolution“, siehe Beniger (1986), nicht wie in der deutschen Debatte Luhmann, siehe S. 1326 ff. Im Ergebnis ist das gleich: Auch bei Schwartz dient Information der Produktion von Entscheidung, siehe S 1333.

[1421] Siehe Schwartz (1992, S. 1343 ff.). Kern der Begründung ist die Behauptung, „[p]rivacy does not help once the issue becomes not *whether*, but *how* personal data should be collected and processed“, siehe S. 1347. Schwartz Konzept von „bureaucratic justice“ ist dabei schlicht „due process“, d. h. Verfahrensgerechtigkeit, und für „human autonomy“ bezieht er sich auf John Stuart Mill sowie Jürgen Habermas' Kritik an der Kolonialisierung der Lebenswelt in seiner Theorie des kommunikativen Handelns, siehe Schwartz (1992, S. 1348 ff.). Eine sehr ähnliche Konzeption findet sich schon bei Bischoff und Burkard (1984) und Bischoff (1984).

[1422] Siehe Schwartz (1992, S. 1374 ff.).

[1423] Eigentlich sogar von einer Dreiteilung, aber – auch wenn sie durchaus Einfluss auf die *privacy-* und Datenschutzdiskussion hatte – die „reine“ IT-Sicherheitsdebatte muss hier aus Platzgründen ausgeklammert werden.

und Praktikerinnen sowie Vertreterinnen aus Verwaltung und Datenschutzaufsichtsbehörden.[1424] Die Tagung ist insofern spannend, weil sie zum Zeitpunkt zweier Umbrüche stattfand – dem durch das Volkszählungsurteil ausgelösten Umbruch im Datenschutzrecht und dem durch den PC ausgelösten Umbruch in Organisation und Praxis der Informationsverarbeitung – und damit sowohl auf die überkommenen – und die übernommenen oder nicht übernommenen – Vorstellungen der vorhergehenden wie auf die Erwartungen an die kommende Epoche verweist. So geht Peter Paul Spies in seinem wohl als Einleitungsbeitrag fungierenden Artikel davon aus, dass „die wesentliche gesellschaftspolitische Forderung die nach einem Regelsystem für den Umgang mit dem Gut Information" sei und damit – begründungslos – quasi Schutzgut und Regelungsgegenstand gleichsetzt.[1425] Dieses Regelsystem operationalisiert er dann für „gesellschaftliche und technische Systeme" als „Menge von Regeln, durch welche die Konflikte in einem System aufgelöst werden", d. h. als „*Recht* des Systems", und statuiert dann: „Wenn das Recht für ein System festgelegt ist und wenn alle Komponenten des Systems den Rechts-Regeln entsprechend konstruiert sind oder werden (d.h. das Recht durchgesetzt ist), dann sind alle Konflikte für das betrachtete System gelöst; wir nennen ein entsprechendes System dann sicher."[1426] Während er die Ableitbarkeit zutreffend nur in einer Richtung als gegeben ansieht – damit folge aus (der Einhaltung von) „Daten-Recht" nicht auch (die Einhaltung von) „Informations-Recht" –, finden sich keine Ausführungen zur dadurch entstehenden Schutzlücke bei (tendenziell) jeder Transformation von „Informations-Recht" in „Daten-Recht". Auch David Chaum legt sein Gestaltungsziel offen – weil die Beziehung zwischen Organisation und Individuen in einer Art gestaltet sei, „which requires individuals to identify themselves in relationships with organizations" und damit „allows records of all an individual's relationships to be linked and collected together into a dossier or personal profile" schlägt er einen Mechanismus vor, der „prevents linking of such data, by allowing individuals to conduct relationships under different account numbers or »digital pseudonyms«", d. h. Transaktionspseudonyme – und unterlässt zugleich eine Auseinandersetzung zu den aus seiner Betrachtung ausgeschlossenen Aspekten, etwa der Frage, welche Inhalte in der Kommunikation zwischen Individuum und Organisation übertragen werden und wie die Organisation auf dieser Basis über das Individuum entscheidet.[1427] Dass schon die Darstellung von zugrunde gelegten Annahmen und verfolgten Regelungszielen eine Herausforderung darstellen kann, zeigen die Ausführungen des ersten Landesdatenschutzbeauftragten von Berlin, Hans-Joachim Kerkau, der dabei nicht sauber zwischen Datenschutz, Datenschutzrecht und Da-

[1424] Siehe den Tagungsband Spies (1985a). Die ausschließlich auf IT-Sicherheit gerichteten Vorträge werden nachfolgend nicht betrachtet, selbst dann nicht, wenn sie behaupten, sich mit dem „Datenschutz" zu beschäftigen. Siehe etwa Heider (1985, S. 73), dessen „Datenschutz" nur „Missbrauchsschutz" gegen eine „Kenntnisnahme sensitiver Informationen" ist.

[1425] Siehe Spies (1985b, S. 2).

[1426] Siehe Spies (1985b, S. 4). Je nach Ebene unterscheidet er dann noch „Informations-Recht" (in sozialen Systemen), „Daten-Recht" (in Systemen, in denen die Informationen schon in Datenform abgebildet wurden) und ein Recht von „Datenobjekten" (in Rechensystemen, d. h. „technische Systeme zur Speicherung und Verarbeitung von Informationen [durch] Speicherung und Verarbeitung von Daten"), siehe S. 5 ff.

[1427] Siehe Chaum (1985a). Chaums Zusicherung, dass „even the tapping of all communication channels and the cooperation of all organizations does not allow messages to be traced to an individual" (S. 33), geht deshalb an mindestens einem Teil des Problems komplett vorbei. Ähnlich sind die Ansätze von Andreas Pfitzmann, der sich – von der Zusammenfassung am Anfang des Artikels abgesehen, wo er auch „vom Kommunikationspartner" spricht – ausschließlich dem Schutz vor Kommunikationsdiensteanbietern, Herstellern *und deren Personal* widmet, siehe Pfitzmann (1985), Günter Höckel und Pfitzmann sowie von Michael Waidner und Pfitzmann, die explizit oder implizit den Kommunikationsinhalt von der Betrachtung ausschließen, siehe Höckel und Pfitzmann (1985) und Waidner und Pfitzmann (1985), das zurückgeht auf Waidner (1985). Zur Terminologie im Bereich Anonymität, Unbeobachtbarkeit und Pseudonymität siehe auch Pfitzmann und Köhntopp (2001).

tenschutzgesetzen trennt.[1428] So unterstellt er dem BDSG etwa, wie das Hessischen Datenschutzgesetz von 1970 auf einem Bild der Datenverarbeitung zu basieren, „das sich an der industriellen Fertigung orientierte und den Aufbau von »Datenverarbeitungsfabriken« mit großen Informationssystemen zum Ziele hatte".[1429] Auch fasst er die Normativität von Recht falsch als „falsche" Beschreibung von Wirklichkeit, wenn er etwa die gesetzliche Verantwortungszuweisung an die „speichernde Stelle" dafür kritisiert, dass damit die „Systemverantwortlichkeit in Netzen und bei verteilter Verarbeitung" nicht abgebildet werden könnte, oder ignoriert einfach, *was offensichtlich seiner Meinung nach nicht sein darf.*[1430] Vor dem Hintergrund seiner Problemanalyse schlägt er als Lösung vor, „durch größere Technikferne, d.h. durch einen höheren Abstraktionsgrad, der wechselnden Technik besser gerecht zu werden" und darüber hinaus das BDSG in Richtung „einfache[r], bürgerverständliche[r], inhaltliche[r] Grundsätze der Datenverarbeitung" zu reformulieren – mit Verweis auf das „Gebot der fairen Datenverarbeitung" im britischen Datenschutzgesetz.[1431] Hans-Jürgen Leib hingegen weist darauf hin, dass sich aus der bisherigen Datenschutzdiskussion keineswegs eindeutig ableiten lasse, „welches Bild von Automation und Kommunikation dem jetzigen Datenschutzrecht zugrundeliegt", weil abgesehen von dem von Steinmüller und Kolleginnen vorgelegten Gutachten insbesondere in den Gesetzesbegründungen und anderen Parlamentsmaterialien dazu „nur wenige und sehr pauschale Ausführungen" gemacht würden.[1432] Sein Ziel ist zu prüfen, ob „neue (verschärfende) Regelungen innerhalb des jetzigen Regelungskonzeptes erforderlich" seien oder ob es eines „grundsätzlich neue[n] Regelungskonzept[s]" bedürfe. Dazu versucht er mangels Explizierung, die „Struktur von Datenverarbeitung, die dem Datenschutzrecht zugrundeliegt", aus den Regelungen selbst zu schließen, allerdings verwechselt auch Leib Normativität und Deskription – „[j]ede Datenverarbeitung ist in sich abgeschlossen und damit beschreib- und identifizierbar"[1433] muss, weil es sich um ein normatives Konzept handelt, eigentlich lauten: Jede Datenverarbeitung muss in sich abgeschlossen und damit beschreib- und identifizierbar sein.[1434] Während Leib nun durchaus Kontrollprobleme in der Praxis sieht, sieht er jedenfalls keine Notwendigkeit für ein grundlegend neues Regelungskon-

[1428] Datenschutzrecht umfasst dabei für Kerkau nicht nur die Datenschutzgesetze, sondern auch die gesamte Rechtsprechung.

[1429] Siehe Kerkau (1985, S. 84). Den Beweis dafür tritt er nicht an, obwohl er das mehrmals in seinem Text ankündigt, siehe etwa S. 86 mit Verweis auf nachfolgende und S. 87 mit Verweis auf vorhergehende Ausführungen. Was er nur zeigt, ist die unsinnige Beschränkung des Gesetzes auf in Dateien gespeicherte Informationen und auf bestimmte, im Gesetz definierte Phasen, siehe S. 87 ff. Letzere ist vor dem Hintergrund der Phasenkonstruktion sinnwidrig, siehe Steinmüller et al. (1971, S. 57 ff.), jedoch durch die Einführung einer Nutzungsphase als „catch all" nicht mehr aktuell, siehe § 3 Abs. 5 BDSG.

[1430] Siehe Kerkau (1985, S. 89 f.). Das Problem ist u. a., dass er aus unerfindlichen Gründen unterstellt, dass es nur *eine* speichernde Stelle gebe (S. 89, Hervorhebung im Original). Und wenn das Gesetz unterstellt, dass „mit der Einrichtung eines On-line-Anschlusses alle Daten als übermittelt gelten", dann sind auch nicht „alle On-line-Anschlüsse mangels Erforderlichkeit rechtswidrig", sondern nur die erforderlichen „On-line-Anschlüsse" zulässig. Daher ist Kerkaus Behauptung, dass das Gesetz für die Zulässigkeit von „On-line-Anschlüssen" „keinerlei Kriterien" (S. 90) enthalte, auch falsch – nur scheint das Ergebnis ihm eben nicht zu gefallen, genauso wenig wie dem Gesetzgeber, der darum zu dieser Zeit schon eine Änderung der Regelung anstrebte, siehe Schmidt (1986).

[1431] Siehe Kerkau (1985, S. 91 ff.).

[1432] Siehe Leib (1985, S. 218). Leibs Forderung nach einer Explizierung der dem Datenschutzrecht zugrunde gelegten Vorstellungen hebt sich so wohltuend von den vielen anderen Arbeiten ab, in denen die Autorinnen ihre eigenen (Fehl-)Vorstellungen dem Datenschutzrecht unterschieben, dass es eine Schande ist, dass seine Arbeit so wenig Beachtung findet, siehe auch Pohle (2011) und Pohle (2014b, S. 91, Rn. 13 Fn. 23).

[1433] Siehe Leib (1985, S. 222).

[1434] Und genau so *fordert* es auch Steinmüller, etwa in Steinmüller et al. (1978, S. 98 ff.) als „Postulat III: Abschottung des riskanten Informationssystems", und *beschreibt* es nicht einfach nur.

zept, die Behauptung allerdings sofort wieder einschränkt, „weil ein anderes Regelungskonzept – das diesen Problemen wirksam begegnen kann – nicht in Sicht ist."[1435] Karl Rihaczek hingegen verweist tatsächlich auf eine der Annahmen, die dem Datenschutzrecht zugrunde liegen: „Das BDSG geht offensichtlich von der Annahme aus, daß Datenverarbeitungssysteme dem Willen ihrer Herren vollkommen unterworfen sind und sich nicht gegen ihn sichern lassen."[1436] Für die Rechtsgestaltung folge daraus eine starke Selbstbeschränkung, die er überwinden wolle, denn es gebe „durchaus Systeme [...], die sich dem unlauteren Willen ihrer Herren versagen."[1437] Er verlangt nun nach Systemen, die „Mißbrauch vom ordentlichen Gebrauch unterscheiden und wohlunterschieden verhindern können", zeigt davon allerdings ein sehr mechanistisches Verständnis, wenn er etwa meint, dass „man Datenverarbeitung auch praktisch unkorrumpierbar (manipulationssicher) gestalten" könne, und am Ende auch nur bei Berechtigungskontrollsystemen landet.[1438] Ähnlich ambivalent sind die Ausführungen Steinmüllers zur Frage der sozialen Beherrschbarkeit offener Netze, d. h. Netze mit offener Nutzerinnen- und Zweckstruktur, die er für grundsätzlich erreichbar hält, jedoch von einer Sozialverträglichkeit abgrenzt.[1439] Seine Lösungsvorschläge zielen erstens auf die Schaffung einer „[b]etroffenenrelevanten Systemtransparenz" durch technische, organisatorische und rechtliche Mechanismen[1440] und zweitens auf die Reproduktion von dezidierten Netzen im offenen Netz zur Lösung des Problems der offenen Zweckstruktur durch Rückgriff auf die Erfahrungen aus dem Datenschutzrecht: ein Verbot der sozial ungeregelten „Teletransaktionen" mit Erlaubnisvorbehalt.[1441] Voraussetzung für die Erlaubnis ist dann der Nachweis sozialer Beherrschbarkeit durch die Betreiberin.[1442] Damit würde die Lösung des Problems operationalisiert, mithin ein grundsätzlich unlösbares Problem aufgeteilt und auf der Zeitachse verteilt, „wobei die jeweils ungelöste Restmenge in die Zukunft geschoben wird."[1443] Das Gegenteil zu diesen eher breit *und gesellschaftlich* gedachten Ansätzen präsentieren Reinhard Gotzhein und Lothar Horbach in ihrer Analyse des Erlangener Krebsregisters, indem sie ein Rechtekontrollsystem und dessen technische Umsetzung als zur Erfüllung der gesetzlichen Anforderungen hinreichend postulieren.[1444] In diese Falle von durch Technikerinnen selbst (fehl-)interpretierte rechtliche Anforderungen und deren (mechanistische) Ableitung

[1435] Siehe Leib (1985, S. 223 ff., 225).
[1436] Rihaczek (1985, S. 232).
[1437] Rihaczek (1985, S. 232).
[1438] Siehe Rihaczek (1985, S. 233).
[1439] Siehe Steinmüller (1985b). Seine Unterscheidung von sozialer Beherrschbarkeit und Sozialverträglichkeit legt er am Beispiel des Straßenverkehrs dar, der durch Verkehrsregeln und Infrastrukturgestaltung sozial beherrscht sei, allerdings wegen der gesellschaftliche wirksamen Sekundärfolgen – etwa im Umweltbereich – nicht sozialverträglich (S. 239 f.). In einer etwas weniger soziologisierten Form operationalisiert Ulrich Seidel das Gebot der sozialen Beherrschbarkeit im „Grundsatz der Prüfbarkeit", siehe Seidel (1984, S. 191), .
[1440] Siehe Steinmüller (1985b, S. 243 f.). Technisch soll das durch Protokollerweiterungen, organisatorisch durch die Institutionalisierung einer an die Institution der Datenschutzbeauftragten angelehnten „Netzbeauftragten" und rechtlich durch den Ausbau des Telekommunikationsrechts geschehen. Die Rolle der Netzbeauftragten ist dabei sehr problematisch, weil Steinmüller ihr zugleich als „einer einzigen gesellschaftlichen Instanz" die Aufgabe zuweisen und gestatten will, gegen den Willen der Beteiligten Kommunikationen zu entschlüsseln, etwa zur Ermöglichung von Strafverfolgung in bestimmten Fällen, ohne dabei die Folgen der Zuweisung solch fundamental widersprüchlicher Aufgaben an die gleiche Stelle zu reflektieren. Siehe dazu etwa die umfassende Diskussion über die Rolle des BSI im Hinblick auf die Prüfung von „Bundestrojanern".
[1441] Siehe Steinmüller (1985b, S. 244 ff.). Teletransaktionen sind dabei „telekommunikationsgestützte soziale Interaktionsmuster", im Gegensatz zum formalen „Dienst"-Begriff der damaligen Bundespost spricht Steinmüller auch von „inhaltlichen Telediensten" (S. 245).
[1442] Siehe Steinmüller (1985b, S. 246).
[1443] Siehe Steinmüller (1985b, S. 246).
[1444] Siehe Gotzhein und Horbach (1985).

in technische Anforderungen tappt Fritz Krückeberg gerade nicht, sondern fordert überhaupt erst einmal die Entwicklung von geeigneten Prüf- und Zertifierungskonzepten zur Sicherstellung von Datenschutz(rechts)konformität von Software in Verbindung mit dem System, auf dem sie läuft, nicht jedoch der Hardware, und deren anschließende Einführung.[1445]

Einen Schritt weiter als Krückeberg geht Herbert Burkert, der fordert, überhaupt erst einmal technische „Gestaltungsanforderungen aus der rechtlichen Diskussion" abzuleiten.[1446] Grundlegend sei dafür der im Datenschutzrecht zentrale Begriff des Verwendungszwecks, der zusammen mit Umfang und möglicher Weiterverwendung von personenbezogenen Informationen gesellschaftlich, d. h. mindestens zwischen „Informationsgeber" und „Informationsnehmer", ausgehandelt werden müsse mit der Folge, dass das zu implementierende System sich an diese Aushandlungsergebnisse zu halten habe, zugleich es aber wiederum ermöglichen müsse, „einen erreichten Konsens, wenn erforderlich, zu überprüfen und Zustimmungen zurücknehmen zu können."[1447] Als Anforderungen an die Gestaltungsverfahren identifiziert Burkert die Möglichkeit der umfassenden Darstellbarkeit des Systems mit dem Ziel der Sicherstellung der Überprüfbarkeit der Anforderungserfüllung, die Aufrechterhaltung der Gestaltbarkeit des Systems zum Zeitpunkt seines Einsatzes sowie die Möglichkeit einer vollständigen Thematisierung der Interessen aller Beteiligten,[1448] während er Datenschutz in den materiellen Anforderungen Systemtransparenz, Datenquantität und -qualität, Kontrollierbarkeit – oder besser: Kontrollfähigkeit und Kontrolle – und IT-Sicherheit operationalisiert.[1449] Burkerts Vorschläge etwa zur Transparenzerzeugung haben dabei bis heute nicht an Aktualität eingebüßt: Systeme, die den Betroffenen sowohl ihre eigenen Datenflüsse wie die Verarbeitungsverfahren – „etwa nach welchen Kriterien welche personenbezogenen Informationen für welche Entscheidungen verarbeitet werden" – veranschaulichen, das daraus entstehende Dilemma der für die Sicherstellung der Systemtransparenz im System zusätzlich erzeugten Strukturierungsinformationen, das Problem, wie die Komplexitätsreduktion für die Sicherstellung von Benutzungsfreundlichkeit selbst wiederum daraufhin kontrollierbar bleibt, „daß nicht wichtige Elemente bei diesem Reduktionsprozess ausgeschieden werden", oder der Umgang mit der Gefahr, „daß soziale und politische Verantwortlichkeit für die durch diese Systeme produzierten Entscheidungen verdeckt werden."[1450]

Die Diskussion um die Technikgestaltung wird dabei in den 1980er Jahren stark von einem Programm beeinflusst, das das vom Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen unter dem Titel „Mensch und Technik – Sozialverträgliche Technikgestaltung" aufgelegt und zur Finanzierung von wissenschaftlichen Untersuchungen, Modellvorhaben und Praxisprojekten genutzt wurde.[1451] Unter Verzicht auf eine „objektive Bestimmung und allgemeingültige Wertung des Begriffs Sozialverträglichkeit als Gemeinwohl für alle" wird die

[1445] Siehe Krückeberg (1985).
[1446] Siehe Burkert (1985, S. 11 und Fn. 9).
[1447] Siehe Burkert (1985, S. 12 f.). Letzeres entspricht offenkundig der erst viel später mit einem eigenen Namen versehenen Forderung nach „Intervenierbarkeit", siehe Rost und Pfitzmann (2009). Die Diskussion ist jedoch zu diesem Zeitpunkt keineswegs mehr neu, siehe schon Dette et al. (1979, S. 127 f.) zur Möglichkeit einer Umsetzung in Technik, an die Burkert – zumindest inhaltlich – anschließt, siehe Burkert (1985, S. 24 f.).
[1448] Siehe Burkert (1985, S. 14).
[1449] Siehe Burkert (1985, S. 14 ff.).
[1450] Siehe Burkert (1985, S. 24 f.).
[1451] Siehe von Alemann und Schatz (1987, S. 13 ff.). Die ganze Diskussion wurde vorwiegend von den Sozialwissenschaften getragen, und entsprechend dem verantwortlichen Ministerium und seinem Zuschnitt sowie der das Ministerium besetzenden Partei beschäftigte sich ein wesentlicher Teil der Vorhaben mit der Arbeitswelt in der Informationsgesellschaft, allerdings wurde auch einige Bücher in der Reihe des Programms veröffentlicht, die in den Bereich dieser Arbeit fallen, etwa Koslowski (1988) (Band 3), Roßnagel et al. (1990a) (Band 5), Roßnagel et al. (1990b) (Band 8), Lenk et al. (1990) (Band 10) und Bräutigam et al. (1990) (Band 12).

Verbesserung der „Mitwirkung der Betroffenenseite“ in den Mittelpunkt gestellt,[1452] durch die Einfluss auf die Gestaltung von Technik als einem Produkt gesellschaftlicher und widersprüchlicher Prozesse genommen werden soll,[1453] insbesondere durch die Untersuchung und Gestaltung der Technikentwicklungsprozesse von der Diskussion gesellschaftlicher Ziele über die Analyse von Technikwirkungen und das Erkennen von Gestaltungsspielräumen bis hin zur Entwicklung technischer Alternativen.[1454]

Zwei mehr oder weniger lose Personen- oder Arbeitsgruppen, deren Arbeiten in den Bereich dieser Untersuchung fallen, beteiligten sich an der Debatte um sozialverträgliche Technikgestaltung: eine recht lose Gruppe um Adalbert Podlech an der TU Darmstadt und die „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)“ um Alexander Roßnagel an der Uni Kassel. Während die Darmstädter Gruppe versucht, Datenschutz als Sozialverträglichkeitskriterium zu fassen und zugleich als Technikgestaltungsprinzip,[1455] wird in Roßnagels Umfeld der Begriff der Sozialverträglichkeit schnell durch den der Verfassungsverträglichkeit ersetzt und dieser anstelle eines breiten Datenschutzbegriffes zugrunde gelegt.[1456]

Eine Verfassungsverträglichkeitsprüfung soll dabei in einem Dreischritt ablaufen: erstens Darstellung der normativen Ziele des Grundgesetzes, vor allem „die normativen Versprechen von Freiheit und Gleichheit, Demokratie und Machtbegrenzung“, zweitens Abschätzung der Veränderung von „Verwirklichungsbedingungen von Verfassungszielen“ durch neue Systeme und drittens Untersuchung der Rückkopplung, etwa einen möglichen Änderungsdruck, auf die Verfassung.[1457] Darauf aufbauend versucht Roßnagel, eine Übersicht über Probleme und Bedingungen verfassungsverträglicher Technikgestaltung zu geben, die allerdings noch sehr abstrakt bleiben, wie die Institutionalisierung von Interessenvertretung in Entwicklungsprozessen, das Erstellen von Alternativkonzepten, das möglichst lange Offenhalten von Kontingenzen oder die „Inkorporierung“ von Freiheitsschutz in Technik.[1458] Bei dem etwas später vorgelegten Konzept KORA – „Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen“[1459] – handelt es sich dann um einen vierstufigen Konkretisierungsprozess, der sich auf ein zu entwickelndes soziotechnisches System bezieht: erstens die Transformation von Grundrechten in „grundrechtliche Anforderungen“, indem die Grundrechte auf dieses System hin konkretisiert werden, zweitens deren Ableitung in „rechtliche Kriterien“, bei denen es sich im Grunde um Formen von Schutzzielen handelt, auch weil sie explizit als zueinander in Widerspruch stehend angenommen werden, gerade wie die zugrunde liegenden Interessen widersprüchlich sein können, drittens die Ableitung von „funktionsbezogenen Gestaltungszielen“ aus den Kriterien, wobei die Funktionen immer nur in der Form abstrakter oder abstrahierter „Grundfunktionen“ betrachtet werden, und viertens

[1452] Siehe von Alemann und Schatz (1987, S. 21).
[1453] Siehe von Alemann und Schatz (1987, S. 28 f.).
[1454] Siehe von Alemann und Schatz (1987, S. 39).
[1455] Siehe schon früh Scholz (1988).
[1456] Siehe die Beispiele für gesellschaftliche Folgewirkungen, die zu adressieren seien, bei Roßnagel (1989a), die alle unter den vorher genutzten Begriff des „Datenschutzes im weiteren Sinne“ subsumiert werden können. Dahinter scheint auch die Absicht zu stehen, die zugrunde gelegten Kriterien als gesellschaftlich konsentiert zu markieren, siehe Roßnagel (1989b, S. 239).
[1457] Siehe Roßnagel (1989b, S. 242 f.).
[1458] Siehe Roßnagel (1989b, S. 250 ff.) und ausführlicher Roßnagel et al. (1990b, S. 272 ff.).
[1459] Grundlegend Hammer et al. (1992) und Hammer et al. (1993). KORA ist bis heute Gegenstand von Veröffentlichungen aus dem Roßnagel-Umfeld, siehe etwa Bräunlich et al. (2011) oder Kahlert (2014), ohne dass sie großen Einfluss in der Praxis erreicht haben zu scheint. Siehe auch die Weiterentwicklung NORA, die „normative Anforderungsanalyse“, Hammer (1999) und Hammer (2000).

die Angabe konkreter „Gestaltungsmaßnahmen“ für die Zielerreichung.[1460] Indem die Autoren ihre Ableitung mit den Grundrechten beginnen – und damit im wesentlichen auf der Basis von materiell formulierten Grundlagen – und diese dann in Prinzipien transformieren, umgehen sie zugleich – ob wissentlich oder nicht, ob gewollt oder nicht – das zentrale Grundproblem der Ableitung von Prinzipien aus dem deutschen Datenschutzrecht – und dabei vor allem aus dem BDSG und allen anderen für private Datenverarbeiter geltenden Datenschutznormen –, nämlich dass diese in erster Linie prozedural – und eben nicht materiell – ausgerichtet sind.

Die Alternativkonzeption von Lothar Bräutigam, Heinzpeter Höller und Renate Scholz hingegen beschränkt sich bei der Betrachtung auf das für öffentliche Stellen geltende Recht, in dem die grundlegenden Abwägungsentscheidungen bereits vom Gesetzgeber getroffen und im Gesetz umgesetzt sind.[1461] Die Autorinnen setzen ihr Konzept dabei setzt direkt auf der These auf,

> „[d]ie Einhaltung gesellschaftlich geltenden Informationsrechts muß durch die Abbildung auf in informationstechnischen Systemen geltendes Systemrecht unterstützt werden. Die Systeme dürfen – in ihrem jeweiligen Anwendungskontext – nicht können, was sie nicht sollen.“[1462]

und bleibt viel weniger abstrakt, verliert damit – jedoch sicher auch mit der Selbstbeschränkung auf die relationale Datenbanksysteme – Anschlussfähigkeit für spätere Arbeiten. Für Informatikerinnen faszinierend – und so später nur selten in anderen Projekten zu sehen – beginnen die Autorinnen ihre Untersuchung von technischen Gestaltungsvorschlägen mit einer vertieften Auseinandersetzung mit den gesellschaftlichen und rechtlichen Grundlagen des Datenschutzrechts mit dem Ziel der Durchdringung der Materie in einer Weise, „daß technisch »bedenkbare« Prinzipien und Strukturen erkennbar werden.“[1463] Die Menge der softwaretechnisch realisierbaren „Regelungskonstrukte“ – „allgemeine Regelungsmuster“, „Grundprinzipien“ – nennen sie dann „Systemrecht“ – in Abgrenzung zum „Informationsrecht“, das Menschen und Organisationen adressiert –, und dessen Formulierung ist das Ziel der Arbeit.[1464] Die Trennung zwischen dem technischen und dem soziotechnischen System sorgt auch an einer anderen Stelle für eine grundlegende und sehr sinnvolle Unterscheidung: Informationstechnische Systeme lassen sich nach ihrer „Datenschutzeignung“ klassifizieren, soziotechnische Systeme und deren Informationsverarbei-

[1460] Siehe dazu umfassend Hammer et al. (1993), leider ohne Betrachtung konkurrierender Ansätze – Bräutigam et al. (1990) wird nur *pro forma* zitiert, Steinmüller et al. (1978), Schrempf (1990) oder Gerhardt (1992) gar nicht.

[1461] Siehe zuerst Scholz (1988) und dann ausführlich Bräutigam et al. (1990). Insbesondere können sie sich dabei dann schon auf gesetzlich fixierte Zwecke und Mittel – „Aufgaben“ im Rechtssinne – stützen, siehe Bräutigam et al. (1990, S. 38 ff.) und Podlech (1990, S. 348 f.). Diese Entscheidung machen die Autorinnen allerdings explizit und trennen dazu zwischen der „*strukturelle[n] Abbildung* von informationsrechtlichen Vorgaben auf – *unabhängig vom Anwendungskontext* – softwaretechnisch realisierbare Regelungsmechanismen informationstechnischer Systeme“ und der „*inhaltliche[n] Abbildung* von informationsrechtlichen Normen auf ein konkretes informationstechnisches System *im Anwendungskontext* einer bestimmten datenverarbeitenden Stelle“, um sich dann auf die erste Aufgabenstellung zu beschränken, weil diese ausreiche, um „Regelungsstrukturen zu extrahieren, die technisch unterstützbar sind“, siehe Bräutigam et al. (1990, S. 23).

[1462] Bräutigam et al. (1990, S. 3).

[1463] Siehe Bräutigam et al. (1990, S. 4 f. und 8 ff.). Diese Idee ist allerdings in der Theorie besser als ihre Umsetzung in der betrachteten Studie. Der Vorteil einer solchen Auseinandersetzung mit den gesellschaftlichen und/oder rechtlichen Grundlagen liegt darin, dass diese Auseinandersetzung im Nachhinein als eine gute Grundlage sowohl für interdisziplinäre Anschlüsse, für aufsichtsbehördliche Prüfungen, für Zertifizierungsverfahren wie sogar für eine neu konzeptionierte informierte Einwilligung dienen kann.

[1464] Siehe Bräutigam et al. (1990, S. 25 ff.). Das Konzept des Sytemrechts geht zurück auf Minsky und Rozenshtein (1987).

tungspraxen nach ihrer „Datenschutzkonformität“,[1465] weil den Autorinnen bewusst ist, dass das Systemrecht das Informationsrecht „nicht vollständig technisch abbilden, durchsetzen und kontrollieren“ kann und deshalb „der Einbettung in einen organisatorischen Rahmen [bedarf], der die Bedingungen einer datenschutzkonformen Anwendung [...] formuliert und absichert.“[1466] Als Ankerpunkt für ihre Ableitung wählen die Autorinnen des Zweckbegriff Bernhard Hoffmanns[1467] mit dessen Funktionen: Zwecksetzung diene der Auszeichnung erwünschter Wirkungen und deren Trennung von unerwünschten, sie institutionalisiere „systemeigene Mechanismen der Weltdeutung sowohl bezüglich der Innensicht als auch der Außensicht“ und sie sei strukturbildend, sowohl gegenüber der Umwelt als auch zwischen Teilsystemen, und wirke in „Zweckhierarchien“ als „Parameter auf die Menge zweckerfüllender Mittel, systemkonstituierender Strukturen und das Verhalten der zweckgesteuerten Subsysteme.“[1468] Auf dieser Basis unternehmen es die Autorinnen dann, strukturell verschiedene Prinzipien jeweils in das Systemrecht abzubilden – allgemeine oder spezifische Verarbeitungsbeschränkungen für Nutzerinnen, Rechte der Betroffenen, die diese selbst direkt im System wahrnehmen können, objektive Regelungen wie Protokollierungen, Löschungen nach Zweckerreichung oder Fristablauf sowie die daraus resultierende Benachrichtigung der Betroffenen und nicht zuletzt die Prinzipien von Transparenz und Kontrollierbarkeit, sowohl hinsichtlich des Systems wie der Prozesse – und zugleich Anforderungen an den Transformationsprozess zu formulieren, der „geregelt, verläßlich, demokratisch und transparent“[1469] ablaufen solle.

Im Umfeld des gleichen Projekts „sovt“ untersucht Hans-Jürgen Seelos die Implementation von insbesondere systemdatenschutzrechtlichen Anforderungen in ein computerunterstütztes Krankenhausinformations- und -kommunikationssystem.[1470] Von daher überrascht es wenig, wenn einer der Schwerpunkte seiner Arbeit auf der Frage der Umsetzung einer informationsgewaltenteiligen Systemstruktur sowohl im Technikgestaltungsprozess wie in der Technik selbst liegt, und Seelos dabei sowohl auf die betreffenden Vorarbeiten von Podlech wie die von Steinmüller zurückgreift.[1471] Zu den nicht nur für die Implementierung systemdatenschutzrechtlicher Anforderungen relevanten Ansätzen gehört die Speicherung des Kontextbezugs von Informationen als Attribute – oder Metadaten – der gespeicherten Daten und ihre Nutzung für nachfolgende Entscheidungen *im informationstechnischen System wie auch im soziotechnischen* bis hin zur

[1465] Siehe Bräutigam et al. (1990, S. 29).

[1466] Siehe Bräutigam et al. (1990, S. 33). Das werde deutlich in der Tatsache, dass *in technischen Systemen* grundsätzlich „nur unberechtigte Zugriffe seitens formell nicht Berechtigter, nicht aber materiell unberechtigte Zugriffe formell Berechtigter verhinder[t werden] können“, siehe Bräutigam et al. (1990, S. 77).

[1467] Basierend auf im gleichen Projekt an der TH Darmstadt, „Sozialverträgliche Technikgestaltung (sovt)“, entstandenen Vorarbeiten zu seiner im folgenden Jahr erscheinenden Dissertation Hoffmann (1991).

[1468] Siehe Bräutigam et al. (1990, S. 46). Siehe dazu umfassend – und bis heute nicht wieder erreicht – Hoffmann (1991) und mit weiteren Nachweisen Pohle (2015b). Siehe zur Frage der „Weltdeutung“ im Sinne der Modellierung sowie zur Modellierungshoheit auch Pohle (2016c).

[1469] Siehe Bräutigam et al. (1990, S. 148 ff.). Siehe zum Vorschlag einer Umsetzung von Betroffenenrechten – über § 9 BDSG, wonach die verantwortlichen Stellen „die technischen und organisatorischen Maßnahmen zu treffen [haben], die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes [...] zu gewährleisten“ – in Technik Wächter (1996). Siehe zur historischen Einordnung dieser Regelung und den damit verspielten Chancen für eine datenschutzfreundliche Technikgestaltung Pohle (2015a).

[1470] Siehe Seelos (1991).

[1471] Siehe zu den Vorarbeiten insbesondere Podlech (1976b), Podlech (1982), Steinmüller et al. (1978) und Steinmüller (1990). In die gleichen Fußstapfen wird wenig später auch Matthias Nodorf treten, der wie Seelos bei Podlech promovierte, und diesen Ansatz für die Technikgestaltung im Bereich computergestützter Verwaltungstätigkeiten im System der gesetzlichen Krankenversicherung zu nutzen, siehe Nodorf (1995).

Aggregation, die darum in einem solchen System – im Gegensatz zu vielen heute diskutierten Systemen – gerade nicht als kontext- oder zweckfrei erscheinen können.[1472]

Zwar werden diese Vorarbeiten durchaus von Simone Fischer-Hübner zitiert, aber gerade dort, wo ihre eigenen Vorschläge quasi deckungsgleich sind mit jenen aus diesen Vorarbeiten, fehlen Quellenangaben:[1473] So übernimmt sie zwar die Aufgabenbasiertheit des Entscheidungsmodells über Informationsverarbeitungen, das gerade ihr zentraler Ansatz sein soll, ein „Task-Based Privacy Model", aus den Vorarbeiten, diese Vorarbeiten werden jedoch nur allgemein als vergleichbare Arbeiten aufgeführt oder nach der Darstellung des Modells im Rahmen eines Beispiels erörtert.[1474] Als zentrale Differenz wird dann die Entwicklung eines „formal state machine model with formal proofs that all state transition functions preserve all defined privacy properties" angegeben,[1475] das auf Betriebssystemebene umgesetzt werden soll. Obwohl sie – ebenso wie ihr Habilitationsbetreuer Klaus Brunnstein – beteuert, dass sie mit der Arbeit versuche, datenschutzrechtliche Anforderungen in technische zu übersetzen, sind die von ihr aufgeführten Prinzipien bei weitem nicht vollständig: Neben den klassischen IT-Sicherheitsschutzzielen *confidentiality*, *integrity* und *availability* betrachtet sie nur die *privacy*-Aspekte *anonymity*, *pseudonymity*, *unobservability* und *unlinkability* und darüber hinaus die datenschutzrechtlichen Prinzipien Zweckbindung und Erforderlichkeit.[1476] Alle weiteren datenschutzrechtlichen Anforderungen werden ignoriert, auch die in den Vorarbeiten betrachteten – wie Betroffenenrechte oder Transparenzpflichten –, für die dort sogar Umsetzungvorschläge vorgelegt wurden.[1477]

Steinmüller versucht Anfang der 1990er Jahre – zum damit zugleich beginnenden Ende seiner akademischen Laufbahn[1478] –, alle seine Erkenntnisse in einer „*Summa Informatiae*"[1479] zusammenhängend darzustellen – unter Umbennenung des „Datenschutzes im weiteren Sinne" in „Informationsschutz", „die Menge aller Maßnahmen, die die politische und private Freiheit des einzelnen wie von machtunterlegenen Gruppen und anderen gesellschaftlichen Kräften angesichts der Informationssysteme gewährleisten", denn das Probleme bestehe „in der Freiheitsbedrohung durch die den Bürger und Werktätigen zum Verarbeitungsobjekt machende Verdatung, dem das zu kontrollierende Informationssystem mit seinen [sozialen wie technischen] Komponenten gegenübertritt".[1480] Als positive Gestaltungskriterien aus Datenschutzsicht formuliert er zehn „Transparenzgebote", wobei er einen sehr weiten Begriff von „Transparenz" hat, den er auch hätte „Schutzziel" nennen können: (1) das Postulat der ökonomischen Realisierung, (2) das

[1472] Siehe Seelos (1991, S. 40 ff.).

[1473] Siehe Fischer-Hübner (1994), Fischer-Hübner und Ott (1998) und umfassend Fischer-Hübner (2001).

[1474] Siehe zum ersten Fischer-Hübner (2001, S. 161 ff.) die Hinweise auf Bräutigam et al. (1990) und zum zweiten Fischer-Hübner (2001, S. 198) den Hinweis auf Seelos (1991).

[1475] Siehe Fischer-Hübner (2001, S. 161).

[1476] Siehe Fischer-Hübner (2001, S. 36 ff., 107 ff., 156).

[1477] Das wirft einen zentralen Punkt auf, der in der Debatte bislang komplett übersehen wird – überraschenderweise nicht nur von Informatikerinnen, sondern auch von Juristinnen: Solange die informatischen Ansätze nicht nachweisen, dass sie eine vollständige Abdeckung des – jedenfalls für die verantwortliche Stelle geltenden – Datenschutzrechts leisten (oder mindestens die Differenzen zu einer vollständigen Abdeckung nachweisen), sodass der (angemessene) Einsatz eines solchen Ansatzes (unter definierten Bedingungen und innerhalb festgelegter Grenzen) sowohl notwendig wie hinreichend für die Erfüllung datenschutzrechtlicher Anforderungen ist, werden solche Ansätze sich nicht in der Praxis durchsetzen, denn insbesondere private Akteurinnen müssen in einer bürgerlichen Rechtsordnung nur eines nachweisen: Rechtstreue.

[1478] Siehe dazu die Beiträge in Garstka und Coy (2014), insbesondere Coy (2014).

[1479] Coy (2014, S. 94).

[1480] Siehe Steinmüller (1993), zur Umbennenung S. 670 f, zur Problembeschreibung S. 676. In der vorliegenden Arbeit wird dafür weiter durchgehend der Begriff „Datenschutz" genutzt. Zumindest gehört Steinmüller zu den wenigen Juristinnen – obwohl er ja auch Informatiker war –, die sauber zwischen Datenschutz und Datenschutzrecht trennen, siehe S. 671.

Postulat der technischen Realisierung (gegenüber rechtlichen oder organisatorischen), (3) das Postulat der Abschottung, (4) das Postulat des ausgeschlossenen Dritten, (5) das Postulat der definierten Struktur (zur Sicherstellung von Voraussehbarkeit), (6) das Postulat der Einfachheit (eigentlich: Minimierung), (7) das Postulat der differenzierenden und verteilten Kontrolle, (8) das Postulat der doppelten Kontrolle (intern wie extern), (9) das Postulat des zusätzlichen Schutzes (gegenüber herkömmlichen, oder „analogen", Systemen) und (10) das Postulat der Beteiligung der Betroffenen.[1481] Die meisten dieser Aspekte werden von der Kerninformatik – vielleicht besser: Schmalspur-Informatik – ignoriert.

Die Kerninformatik fokussiert sich vor allem auf Anonymität und Anonymisierung als Schutzmechanismen sowie möglichen Angriffen auf Anonymität, etwa durch die Möglichkeit der Re-Identifizierbarkeit anonymer oder anonymisierter Informationen. Die Debatte wird dabei wesentlich von den Vorschlägen von David Chaum geprägt, in der Bundesrepublik auch von Andreas Pfitzmann. Beide stützen sich auf die auch in anderen Disziplinen – sowie in der öffentlichen Debatte – allgemein vertretene Position, ein Datenschutzeingriff bzw. ein Eingriff in die *privacy* könne nur dann vorliegen, wenn personenbezogene Informationen verarbeitet werden. Daraus folgern sie, dass die Verhinderung der Herstellbarkeit eines Personenbezugs eine Lösung des *privacy-* bzw. Datenschutzproblems sei und schlagen daher entsprechende Systemgestaltungen vor.

Chaum publiziert dazu 1981 einen Vorschlag für ein anonymes Kommunikationsnetzwerk, das auf einer Kaskade von Mixen basiert, durch die alle Nachrichten geleitet werden und in denen jeweils die Reihenfolgen der Nachrichten geändert werden. Die zugrunde liegende Technik kann zugleich für unverkettbare digitale Pseudonyme genutzt werden, so dass Menschen sich gegenüber Organisationen nicht identifizieren müssen, um reproduzierbar mit ihnen zu interagieren.[1482] Zugleich würden diese (nutzerkontrollierten) Pseudonyme allerdings auch die Möglichkeit bieten, durch ihr periodisches Wechseln Verkettungen mit veralteten Informationen über die Individuen aufzubrechen[1483] – ein nutzergesteuertes Vergessen auf Seiten der Organisation.

Auch Pfitzmann forscht in dieser Richtung mit dem Ziel eines anonymitätsgarantierenden Netzwerkes.[1484] Ziel sei es, so Pfitzmann, „zumindest einen Teil des Datenschutzes in dem Bereich des Systems zu realisieren, über den ausschließlich der Teilnehmer bzw. eine Teilnehmergemeinschaft verfügt. Dieser Teil des Datenschutzes ist dann nicht einfach per Gesetz aufhebbar."[1485]

[1481] Siehe Steinmüller (1993, S. 590 f.). Eine Ebene höher, also auf der Datenschutzrechtsebene, verweisen dann die Datenschutzprinzipien – „Zweckbindung, Gesetzesvorbehalt, Verhältnismäßigkeit, Erhaltung des Machtgleichgewichts, datenschutzorientierte Gestaltung und Institutionalisierung externer Kontrolle, um Transparenz für Bürger, Parlamente und Gerichte zu erreichen" – auf diese Gestaltungskriterien, siehe Peschek und Steinmüller (1995, S. 272).

[1482] Siehe Chaum (1981). Siehe auch die Folgearbeiten Chaum (1984) und Chaum (1985b), die auch die bundesdeutsche Debatte beeinflusst haben, siehe Chaum (1985a). Siehe darüber hinaus Chaums Feststellung, dass bestehende Systeme dazu dienten, einseitig die Interessen von Organisationen auf Schutz vor Individuen zu sichern, Chaum (1985c, S. 1031). Dieser Aspekt, gegen den die Datenschutzdebatte ja gerade das Konzept Datenschutz setzt, wird in der IT-Sicherheitsdebatte später unter dem Label „multilateral security" oder „mehrseitige Sicherheit" wieder aufgegriffen, siehe etwa Rannenberg et al. (1996) oder Federrath und Pfitzmann (1997), dort allerdings eher in der Form eines Stakeholder-Ansatzes, siehe umfassend Freeman (2004), der *nur auch* die Interessen der Betroffenen schützt, diesen jedoch nicht das Primat einräumt.

[1483] Siehe Chaum (1985c, S. 1042).

[1484] Siehe Pfitzmann (1983).

[1485] Pfitzmann (1983, S. 412). Als Definition des Datenschutzproblems gibt er später an: „Ein Teilnehmer [eines Kommunikationsnetzes] kann durch Beobachten seiner Kommunikation Schaden erleiden", siehe Pfitzmann (1990, S. 3). Die von Pfitzmann betrachteten Angreiferinnen sind dabei fast ausschließlich externe Lauscherinnen oder die Betreiberinnen der Kommunikationsnetze, siehe S. 3 ff. Kommunikationspartnerinnen werden nur dann als Angreiferinnen betrachtet, „sofern diese die Identitäten der Dienstnutzer erfahren", siehe S. 9.

Während diese erste Arbeit Chaums Vorarbeiten noch nicht wahrnimmt, übernimmt Pfitzmann – gleiches gilt aber auch für die anderen Mitglieder seiner Arbeitsgruppe[1486] – bald schon die Chaumschen Ansätze.[1487]

Auf dieser Basis werden in der Folge unter anderem anonymitätsgarantierende und als „privacy enhancing“ bezeichnete Kommunikationsprotokolle und -systeme entwickelt, etwa für E-Mail.[1488]

Darüber hinaus läuft die Diskussion über Anonymität und Identifizierbarkeit im Datenbankbereich weiter, sowohl in Bezug auf die Analyse von Systemen und Datensammlungen darauf, ob sie sich – und unter welchen Bedingungen – deanonymisieren lassen, als auch wie diese Deanonymisierung verhindert werden kann.[1489]

Diese Arbeiten lassen jedoch zugleich ein großes Problem deutlich werden. Die Informatik ist bis heute nicht in der Lage, ihre eigenen – ob selbstgewählten oder von anderen vorgegebenen – Annahmen und die Akteurinnen oder Systemen zugeschriebenen Eigenschaften kritisch zu hinterfragen. Schon mit den Arbeiten von Chaum und Pfitzmann hätte – gerade auch im Vergleich mit den Arbeiten aus dem Bereich der statistischen Datenbanken – deutlich werden müssen, dass ein *privacy-* oder Datenschutz vermittelt über Anonymität deutliche konzeptionelle Grenzen hat:[1490] Anonymität schützt nur vor der Verkettbarkeit von Transaktion(en) mit identifizierbaren – oder wiedererkennbaren – Personen, nicht jedoch vor der Verkettbarkeit von Transaktion(en) und Personen als solchen.[1491] Oder anders: Anonymität schützt die Außengrenzen der Transaktion(en), nicht jedoch vor Gefahren *innerhalb* der Transaktion(en).[1492] Damit ist Anonymität zugleich *in erster Linie* als Datensicherheitsmaßnahme identifiziert und nur in Ausnahmefällen – nämlich in Bezug auf die Verkettbarkeit verschiedener Transaktionen untereinander und das auch nur unter der Bedingung der Ignoranz gegenüber dem Innenbereich der Transaktionen – eine Datenschutzmaßnahme. Ein Beispiel dafür ist das von Pfitzmann als „Sicherheitsproblem“ angesprochene Problem der Verhinderung einer Diensterbringung,[1493] das gerade dann, wenn dies *durch die Kommunikationspartnerin* geschieht, tatsächlich ein Daten-

[1486] Siehe etwa Waidner (1985).

[1487] Siehe Pfitzmann (1985), Pfitzmann et al. (1986), Waidner und Pfitzmann (1987), Burk und Pfitzmann (1989) und seine 1988 abgeschlossene und 1990 veröffentlichte Dissertation Pfitzmann (1990).

[1488] Siehe etwa Linn und Kent (1988) oder der später darauf aufbauende IETF-Standard „Privacy Enhanced Mail (PEM)“, RFC 1421–1424.

[1489] Siehe die Beschreibung eines Angriffs auf „statistische“ Datenbanken unter Kenntnis der Beziehungen zwischen statistischen Variablen und unter Nutzung von korrelationsbasierten Analyseansätzen Palley (1986), Clarkes grundsätzliche Kritik an einem verstärkten Einsatz solcher korrelationsbasierten Ansätze mit den Folgen für die Betroffenen, Clarke (1988, S. 507), sowie umfassend dazu auch Pohle (2014b). Siehe auch die umfassende Studie des Projekts AIMIPH („*a*nonyme *i*ntegrierte *Mi*krodatenfiles der Bundesdeutschen *P*rivat*h*aushalte“) zur Frage operationalisierbarer Kriterien für die Anonymität von Einzelangaben am Beispiel von umfassenden statistischen Daten der Gesellschaft für Mathematik und Datenverarbeitung, Paaß und Wauschkuhn (1985).

[1490] Das Problem liegt eigentlich auf einer noch viel tieferen Ebene: In den meisten Theorien und Konzepten wird nicht deutlich gemacht, ob die Beschränkung auf personenbezogene Informationen *per Setzung* zum Teil der Theorie oder des Konzepts gemacht wird oder ob sie nur *als Annahme* zugrunde gelegt wird. In den wenigen Theorien und Konzepten, in denen das expliziert wird, ist die Beschränkung auf personenbezogene Informationen eine Setzung, auch wenn sie nie begründet wird. In diesen Fällen aber ist Anonymität eine Lösung des von der Theorie oder dem Konzept beschriebenen Problem. Ist die Beschränkung allerdings nur das Produkt der zugrunde gelegten Annahmen, dann ist Anonymität nur dann eine Lösung, *wenn die Annahmen korrekt sind*.

[1491] Siehe dazu die Ausführungen bei Hansen (2008).

[1492] Ein alternativer Begriff für Transaktion, der zugleich deutlich macht, dass es auch um einen längeren Zeitraum gehen kann, ist Sitzung.

[1493] Siehe Pfitzmann (1990, S. 3).

schutzproblem ist: Wenn die Kommunikationspartnerin die Kommunikation verweigert, weil die Betroffene anonym kommuniziert, dann schützt Anonymität gerade nicht.[1494] Allgemeiner: Soweit Transaktion – technisch oder nicht – stabilisierte soziale Kommunikation, etwa zwischen Google und einer Google-Nutzerin, und zugleich Information ist, können die Kommunikationspartnerinnen die Transaktion selbst als Grundlage für Entscheidungen über die jeweils anderen Beteiligten verwenden, weil sie in der hinreichend großen Erwartung einer sicheren Adressierbarkeit der jeweils anderen Kommunikationspartnerin agieren können, für die Identifizierbarkeit der Kommunikationspartnerinnen gerade nicht Bedingung ist.[1495] Die Frage muss hier offen bleiben, ob der sehr weite Begriff des Personenbezugs bei Steinmüller, der von einer Feststellung von Personenbeziehbarkeit nur innerhalb von Informationssystemen ausgeht, denn auch der Personenbezug sei nur relativ, „nämlich bezogen auf die spezifische Leistung, Benutzer- und Interessenstruktur des jeweiligen Informationssystems“,[1496] hier eine Lösung dieses Problems darstellen könnte. Einerseits könnte mit Steinmüller die oben genannte Google-Nutzerin *für Google* als Betroffene im Sinne des Datenschutzrechts bezeichnet werden, andererseits werden damit jedoch zwei weitere Probleme noch nicht adressierbar: Entscheidungen auf der Basis von statistischen Aussagen *über alle* und Entscheidungen auf der Basis von simplen sigmatischen Fehlzuschreibungen.

Solange dieses fundamentale Problem in der Debatte gar nicht reflektiert wird, kann für den allgemeinen Fall, d. h. ohne Kenntnis des konkreten Informationssystems, nicht einmal sinnvoll entschieden werden, ob und inwieweit sowohl die Betroffenen und ihre Grundrechte wie auch die Funktionsbedingungen der modernen Gesellschaft selbst unter den Bedingungen der modernen Informationsverarbeitung geschützt sind, wenn und insoweit Informationen über Betroffene anonymisiert werden und die eingesetzten informationstechnischen Systeme die Nicht-Deanonymisierbarkeit garantieren. Damit wird auch klar, dass die sich mit der gesellschaftlichen Funktion – oder den Funktionen – von Anonymität, der Frage nach einem Recht auf Anonymität sowie der gesellschaftlichen Auseinandersetzung um Anonymität beschäftigenden Arbeiten[1497] allenfalls Anonymität *als notwendige Bedingung* von *privacy* oder Datenschutz, nicht jedoch auch *als hinreichende Bedingung* beschreiben, analysieren und nachweisen. Über Grenzen von Anonymität wird also nur dann gesprochen, wenn es um die Gefahren einer möglichen Deanonymisierung geht,[1498] gerade nicht jedoch im Sinne von Grenzen von Anonymität als Schutzmechanismus allgemein oder für Klassen von Schutzgütern, denn erst vor dem Hintergrund konkreter Schutzgüter wird entscheidbar, ob Anonymität zu deren Schutz notwendig *und* hinreichend ist. Dieses Versagen wirft zugleich ein Schlaglicht auf die zweifelhafte Qualität der gesamten – nicht nur informatischen – *privacy*-, *surveillance*- und Datenschutzdebatte: Obwohl die übergroße Mehrheit der in diesem Bereich vertretenen Theorien und Konzepte in ihren jeweiligen Begründungszusammenhängen auf einen *funktionalen Zusammenhang* zwischen

[1494] Siehe dazu auch die Diskussion zu dem von Marit Hansen angesprochenen Fall in Pohle und Knaut (2014, S. 218, Rn. 35 und S. 225, Rn. 53 ff.) sowie umfassend Pohle (2016b).

[1495] Das klassische Beispiel dafür ist natürlich eine Interaktion in der analogen Welt, in der nämlich Menschen auch dann aufeinander reagieren können, wenn sie sich nicht namentlich kennen. Siehe auch Manske (2016) dafür, dass in solchen Fällen auch Entscheidungen über das Gegenüber getroffen und dann auf dieser Basis auch gegen das Gegenüber gehandelt werden kann: „Weil sie bei den Braunkohle-Protesten in der Lausitz einen Polizisten verletzte, ist eine Aktivistin zu einer zweimonatigen Haftstrafe verurteilt worden. Die Verletzung war zwar nur ein blauer Fleck, das Cottbuser Gericht urteilte trotzdem vergleichsweise hart – auch weil die Frau sich über ihre Identität ausschweigt.“

[1496] Siehe Steinmüller et al. (1978, S. 85).

[1497] Siehe etwa Lee (1996), Bizer (2000), Rötzer (2000), Rost (2003a) und Rost (2003b).

[1498] Siehe etwa Pfitzmann (2000) und Ohm (2010).

Verarbeitung bzw. Nichtverarbeitung personenbezogener Informationen und einem Schutzgut – oder Schutzgütern – verweist,[1499] wird mit Identifizierbarkeit und Anonymität umgegangen, als seien sie Selbstzwecke.[1500] Und David Phillips, der als einer der sehr wenigen die Konstruktion von Identifizierbarkeit im Recht – jedenfalls in Bezug auf das *amerikanische* Recht mit dem dort weitverbreiteten Konzept der „personally identifiable information" – problematisiert, bleibt erstens bei einer relativ oberflächlichen Analyse stehen, zieht zweitens keine Konsequenzen, die über die damals schon in anderen als dem amerikanischen Rechtsraum hinaus implementierten Aspekte hinausgehen, und ist drittens – jedenfalls mit seiner Problematisierung der Identifizierbarkeitskonstruktion – anschließlich ignoriert worden.[1501]

Daneben gibt es jedoch eine Reihe weiterer Probleme, die in der Debatte grundlegend ignoriert werden und die auch kein gutes Licht auf die disziplinären und interdisziplinären Debatte werfen. So geht etwa die gesamte Anonymitätsdiskussion im Datenbankenbereich davon aus, dass die Betreiberin der Datenbank nicht als Angreiferin in Frage komme und dass das Problem im Grunde nur darin bestehe, möglichst große Teile der gespeicherten Daten zu veröffentlichen und zwar in einer Form, in der sie ohne oder mit möglichst wenigen Einschränkungen hinsichtlich ihrer statistischen Aussagekraft nutzbar ist, und zugleich Dritte – *und nur diese* – daraus keine Rückschlüsse auf in der Datenbank gespeicherte Informationen über Einzelpersonen ziehen können.[1502]

Ähnlich sieht die Situation im Bereich der sogenannten „Privacy-Enhancing Technologies" (PET) aus, wobei dort die – offenen oder versteckten – Annahmen sind, dass alle *privacy-enhancing* Maßnahmen erstens durch „eliminating or minimising personal data" erfolgen, weil das Ziel darin bestehe, „unnecessary or unwanted processing of personal data" zu verhindern, und diese zweitens erreicht würden „all without losing the functionality of the information system."[1503] Ob diese Annahmen von allen Beteiligten an der PET-Debatte geteilt werden, ist nicht

[1499] Das beschreibt, was Rule et al. als „*strategic* privacy" – im Gegensatz „*aesthetic* privacy" – bezeichnen, siehe Rule et al. (1980, S. 22).

[1500] Es handelt sich dabei nicht um eine Frage von „richtigem" oder „falschem" Konzept oder „richtiger" oder „falscher" Theorie, sondern um einen Widerspruch in sich, der die Debatte kennzeichnet. Ein ähnlicher Widerspruch findet sich auch in der Debatte um das sogenannte „Privacy Paradox". Beide Widersprüche sind dringend erklärungsbedürftig.

[1501] Siehe Phillips (2001) und Phillips (2004). Die Oberflächlichkeit zeigt sich etwa darin, dass er in *beiden* Texten darauf hinweist, dass er die Rechtsnormen nur als Laie gelesen habe, obwohl drei Jahre zwischen ihnen liegen.

[1502] Siehe etwa Samarati und Sweeney (1998) als Beginn der nachfolgenden Debatte über „k-Anonymity" – Sweeney (2002b), Sweeney (2002a), Bayardo und Agrawal (2005) –, „l-Diversity" – Machanavajjhala et al. (2007) – sowie „t-Closeness" – Li et al. (2007). Zwar gibt es auch ein paar kritische Worte, siehe etwa Domingo-Ferrer und Torra (2008) und Bambauer et al. (2013), auch ist zumindest unter den Informatikerinnen, die andere *privacy*- oder Datenschutzkonzepte vertreten, allgemein bekannt, wie beschränkt das *privacy*-Konzept in der Datenbankendiskussion ist – so jedenfalls alle in persönlichen Gesprächen mit dem Autor –, aber weder wird das in der Datenbankendiskussion selbst auch nur angesprochen noch ist das in anderen Disziplinen bekannt, die – wie die Juristinnen – stattdessen davon ausgehen, dass es sich bei den „Lösungen", die der Datenbankbereich bereitstellt, um Lösungen für ihre jeweiligen Probleme handelt – und nicht nur um Lösungen für das Datenbanken-*privacy*-Problem. Anders hingegen „Differential Privacy", siehe Dwork (2006), wo die Systembetreiberinnen durchaus als Angreiferinnen wahrgenommen werden.

[1503] Siehe van Blarkom et al. (2003, S. 3). Grundlegend für das Konzept *unter diesem Bezeichner* van Rossum et al. (1995) sowie die überarbeitete Fassung Hes und Borking (2000). Siehe auch die jeweils aktuellen Übersichten zur Technik bei Goldberg et al. (1997), Goldberg (2002) und Goldberg (2007) sowie die seit 2001 jährlich stattfindenden PET-Workshops bzw. PET-Symposien. Zu den wenigen, die kritisch auf diese sehr beschränkte Vorstellung von *privacy* hinweisen und darauf, dass PETs eben allenfalls eine solcherart beschränkt gedachte *privacy* schützen würde, gehören Herbert Burkert und Felix Stalder, siehe Burkert (1997) und Stalder (2002b). Aber auch diese beiden üben keine Kritik an der Annahme, dass ein solcher *privacy*-Schutz zu erreichen sei, „without losing the functionality of the information system."

ganz klar[1504] – zu sehr handelt es sich bei PET auch um ein leeren Bezeichner, der fast beliebig verwendet werden kann, um „irgendwas mit Technik“ zu bezeichnen[1505] – allerdings eben nur fast: Im Zentrum der Aufmerksamkeit stehen Formen von technisch umgesetzter Anonymität sowie in Technik umgesetzte Verfahren zur Anonymisierung und/oder Pseudonymisierung.[1506] Zentrales Element des Vorschlags ist ein als „Identity Protector“ bezeichnetes Element in einem informationstechnischen System *unter Kontrolle der Betroffenen* zur Verwaltung und Freigabe von Identitätsinformationen wie zur Generierung, Verwaltung und Freigabe von Pseudonymen, die während der meisten Interaktionen der Betroffenen mit dem System zur Informationsverarbeitung und Entscheidungsfindung verwendet werden.[1507] Der „Identity Protector“ erinnert damit an eine Mischung aus einem „Reference Monitor“[1508] und einer technischen Umsetzung von Informationsgewaltenteilung – also nicht nur zwischen Betroffenen und der Datenverarbeiterin,[1509] sondern vor allem auch innerhalb der Teilsysteme auf Seiten der Datenverarbeiterin.[1510] Gleichwohl handelt es sich nicht zwangsläufig um anonymitätsgarantierende Systeme im Sinne von Chaum und Pfitzmann, wie John J. Borking, einer der Erfinder dieses Begriffs, deutlich macht, sondern um technische Umsetzungen des datenschutzrechtlichen Erforderlichkeitsprinzips für „identifying“ Informationen und die beliebige Speicher-, Verarbeit- und Nutzbarkeit von „non-identifying“ Informationen.[1511] Und selbst die Auseinandersetzung um P3P, das „Platform for Privacy Preferences Project“, mit dem Endnutzerinnen-Systeme in die Lage versetzt werden sollten, als Clients in Kommunikationsbeziehungen die Verarbeitungsbedingungen mit den

[1504] Siehe auch die Darstellung der Annahmen bei Seda Gürses, die sich nur teilweise mit den hier genannten überschneiden, Gürses (2010, S. 546 f.). Zum Teil erklärt sich diese Diskrepanz wohl daraus, dass Gürses vor allem Beiträge zu anonymen Kommunikationssystemen zum Gegenstand ihrer Betrachtung macht, siehe etwa Anderson (1996), Dingledine et al. (2001) und Clarke et al. (2001), die auch im Rahmen der PET-Debatte diskutiert werden.

[1505] Für dieses fast schon grenzenlose Verständnis von PET siehe etwa Hansen et al. (2004, S. 35), die damit einfach „the technical answer to social and legal privacy requirements“ bezeichnen. Für Burkert umfassen PETs allerdings auch „organizational concepts“, siehe Burkert (1997, S. 125). Darüber hinaus verweist er in seinem Beitrag auf die Debatte in den 1970er Jahren zur datenschutzfreundlichen Technikgestaltung – „privacy-ensuring technical designs“ –, zitiert dabei Steinmüller (1970, S. 88) und beklagt, dass diese Debatte nur wenig Aufmerksamkeit erregt habe, siehe Burkert (1997, S. 136 und Fn. 13) – ohne Folgen für die nachfolgende Debatte in diesem Bereich, die stattdessen alles als Neuentwicklung aus den 90er Jahren ansieht, siehe etwa Bennett und Raab (2003, S. 154), die die Verpflichtung zur technischen Umsetzung des Datenschutzes als Neuerung im niederländischen Datenschutzrecht ansieht – und jeden Verweis auf die EG-Datenschutzrichtlinie an dieser Stelle unterlässt, aus der das übernommen wurde, geschweige denn wahrnimmt, dass auch diese Regelung selbst schon lange vorher Teil des deutschen Datenschutzrechts war, siehe Pohle (2015a). Siehe als konzeptionelles Gegenstück PITs, „Privacy Intrusive Techniques“, Rotenberg (2001, Rn. 65 ff.), wobei er den Begriff von Roger Clarke, allerdings ohne Quellenangabe, übernimmt.

[1506] Das erklärt wohl auch die schon früh vorhandene Begeisterung der Datenschutzaufsichtsbehörden für PETs, siehe etwa Arbeitsgruppe „Datenschutzfreundliche Technologien“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder (1997). Für einen Überblick über die juristische Debatte siehe von Stechow (2005).

[1507] Siehe van Rossum et al. (1995, 1.6 und 3.1).

[1508] Siehe Anderson (1972, S. 22).

[1509] Dieser Teil wird ausführlich unter dem Label „Identity Management“ diskutiert, vor allem als nutzergesteuertes Identitätsmanagement, siehe Hansen et al. (2004), Camenisch et al. (2005), Clauß et al. (2005) und Camenisch et al. (2011).

[1510] Dafür wurde dann – wenig überraschend in den marktbegeisterten 1990er Jahren – erwartet, dass „der Markt“ entsprechende Technik bereitstellen würde, siehe etwa Agre (1999), aber auch Bäumler und von Mutius (2002). Zum Scheitern dieser Vorstellungen siehe auch Rossnagel (2010).

[1511] Siehe Borking (2001, S. 133).

Servern der Datenverarbeiterinnen auf der Basis maschinenlesbarer „Privacy Policies“ „auszuhandeln“, wurde unter dem Label „PET“ geführt.[1512]

Während damit ein Teil der *privacy*- und Datenschutzdebatte relativ schnell auf den „neuen“ Zug „Internet“ aufsprang, brauchte insbesondere die rechtswissenschaftliche Debatte teilweise bedeutend länger.

2.5 Ubiquitär, mobil, multi-medial – das Internet und der „neue“ Datenschutz

Im Mittelpunkt der juristischen Debatte zwischen Anfang der 1990er und Anfang der 2000er Jahre – bis dann circa 2002 oder 2003 die Anschläge vom 11. September 2001 und deren Folgen der Diskussion ihren Stempel aufdrücken – steht die EG-Datenschutzrichtlinie 95/46/EG[1513] – erst in Begleitung ihrer schweren Geburt,[1514] dann zu ihrer Auslegung und ihrer Umsetzung in nationales Recht und am Ende dazu, ob die jeweiligen nationalen Regelungen akzeptable Umsetzungen der Richtlinie sind und ob die Richtlinie vor dem Hintergrund der gesellschaftlichen Durchsetzung des Internets nicht wieder grundlegend überarbeitet werden müsste.[1515] Insbesondere der letzte Teil kann dabei auf die Ergebnisse einer auch in den Rechtswissenschaften gegen Ende der 1990er Jahre breiter werdenden Debatte über die Folgen des Internets für *privacy* und Datenschutz zurückgreifen.[1516] Insgesamt kommt es zu einem Wechsel des Leitbildes des Datenschutzes in der breiten Debatte: Die Zukunft liege in einem Datenschutz *durch* Technik.[1517]

[1512] Siehe dazu Clarke (1998b), Cranor und Reagle (1998), Cranor (2000a), kritisch Clarke (1998a), Grimm und Roßnagel (2000), Catlett (2000), Electronic Privacy Information Center und Junkbusters (2000) und Rotenberg (2001, Abs. 75 ff.). Siehe jedoch auch Borking und Raab (2001), die P3P als eine der „other technologies for privacy protection“ aufführen, aber nicht unter PET subsumieren. Das Projekt ist wenig überraschend gescheitert, eine ordentliche Analyse dafür gibt es aber nicht. Sarah Spiekermann, die an dem Konzept mitgearbeitet hat und es daher für ganz großartig hält, glaubt, das Scheitern liege in der Obstruktionspolitik der Datenverarbeiterinnen begründet, wie sie dem Autor in einem persönlichen Gespräch am Rande einer Tagung 2012 erklärte. Wahrscheinlich liegt es aber schlicht daran, dass in einer maschinenlesbaren P3P-Policy ein wesentlicher Teil der Verarbeitungsbedingungen, die damit hätten ausgehandelt werden sollen, nicht hätte abgebildet werden können, und da diese Aushandlung jedoch gerade rechtlich gefordert ist, hätten die Datenverarbeiterinnen allein durch den Einsatz von P3P keine Rechtskonformität ihrer Datenverarbeitung nachweisen können. Insofern fehlte es einfach an einem überzeugenden Grund für den Einsatz dieser Technik. Obwohl diese Erkenntnis keineswegs neu ist, siehe etwa Grimm und Roßnagel (2000, S. 160) – P3P könne Regelungen nur beschreiben, aber nicht durchsetzen, und würde nur einige, nicht aber alle gesetzlichen Anforderungen abbilden können –, wird P3P insbesondere in der Informatik immer noch als großer, wenn auch historischer, Erfolg angesehen.

[1513] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, veröffentlicht im Amtsblatt der Europäischen Union Nr. L 281 S. 31–50 vom 23. November 1995.

[1514] Siehe etwa Simitis (Simitis in: 2011, Einleitung, Rn. 203 ff.).

[1515] Es handelt sich dabei, wie Lutterbeck in einem durchaus sehr lesenswerten Beitrag richtig feststellt, um einen Dauerkonflikt, siehe Lutterbeck (1998a) und Lutterbeck (1998b), wobei Lutterbecks fast schon extremistischer Internet-Exzeptionalismus nicht nur rückblickend ziemlich lächerlich wirkt, er damit in dieser Zeit aber leider nicht allein ist.

[1516] Auf die zeitgleich in den USA stattfindende Debatte über eine Pflicht zum Einbau von Verschlüsselungstechnik mit staatlichen Hintertüren – „key escrow“ mit Hilfe des „Clipper Chips“ –, die auch unter dem Titel „Crypto Wars“ bekannt ist, kann hier nur kursorisch verwiesen werden. Siehe dazu etwa Phillips (1997), Lessig (1999, S. 47 ff.), Schneier (2004, S. 240 ff.), Anderson (2008, S. 789 ff.).

[1517] Siehe Ulrich (1996), wobei allerdings die kernigen Behauptungen an keiner Stelle fundiert belegt werden. Siehe aber auch Burkert (1997, S. 136 und Fn. 13), der darauf hinweist, dass dieses Leitbild schon die frühe Datenschutzdebatte geprägt habe.

Grundlegend neue Ansätze zur Problemanalayse, zur Problemlösung und zur Operationalisierung der Problemlösung werden in der Diskussion jedoch nicht vorgebracht. Am deutlichsten wird dies gerade in der EG-Datenschutzrichtlinie, die ein kruder Mix – ein „Flickwerk“[1518] – aus zwei Regelungsarchitekturen ist, die auf einander fundamental widersprechenden Grundannahmen aufbauen: der französische Ansatz der Abstufung von Anforderungen nach einer „Sensitivität“ von Informationen und der bundesdeutsche Ansatz basierend auf der Annahme, dass „Sensitivität“ keine Eigenschaft von Informationen ist.[1519] Aber auch Simitis' wenig informiert, aber dafür umso pathetischer vorgetragene Behauptung, „[z]ur Debatte stehen erneut »Notwendigkeit und Grenzen des Schutzes personenbezogener Daten« – nicht mehr und nicht weniger“,[1520] zeigt, wie sehr sich die Debatte im Kreis dreht und wie immer wieder längst überwunden geglaubte Fehlvorstellungen reproduziert werden – und wie sehr diese vor allem durch die Gleichsetzung von Datenschutz und Datenschutzrecht bzw. Datenschutzgesetzen hervorgerufen oder aufrechterhalten werden, etwa wenn Simitis behauptet, „Datenschutz und Informationstechnologie sind untrennbar miteinander verbunden“, und damit die weitgehende Ablösung der „dinosaurienhaften [sic!] Computer der 70er Jahre“ durch PCs meint.[1521] Was für einzelne – oder viele – Regelungen des Datenschutzrechts korrekt ist, ist es weder zwangsläufig auch für den Datenschutz als solchen noch für die rechtliche Regelungsarchitektur,[1522] und so geht auch Simitis' Schlussfolgerung einer freudigen Fixierung auf in Technik umgesetzte IT-Sicherheitsmaßnahmen – denn fast nichts anderes führt Simitis beispielhaft an – am Problem vorbei: Es geht bei ihm im Grunde nur darum, „den Betroffenen die Entscheidungsmacht über die Preisgabe ihrer Anonymität wiederzugeben.“[1523]

2.5.1 Die „neuen“ Gefahren

Die Gefahren, die in der Debatte in den 1990er Jahren als neu oder zumindest wesentlich gesteigert identifiziert werden, decken einen weiten Bereich ab. Sie reichen von der zunehmenden Überwachung am Arbeitsplatz über die Möglichkeit der Erstellung von feingranularen Bewegungsprofilen, der Verarbeitung von Gendaten und der Entscheidung über Individuen auf der Basis von Gruppenprofilen bis zu vermeintlich ausgewachsenen Techniken der politischen Kontrolle.[1524]

Im Mittelpunkt der Diskussion steht jedoch das Internet, bei dessen Nutzung Menschen Unmengen von Spuren hinterlassen, die gespeichert, verarbeitet und genutzt werden können und werden.[1525] Allzuoft weist dabei allerdings die Beschreibung der – wahrgenommenen – Realität im Netz sowohl hinsichtlich der technischen wie der sozialen Verhältnisse auf eklatante Fehlverständnisse, Fehlannahmen oder Fehlvorhersagen über die zukünftige Entwicklung hin.[1526]

[1518] So die französische Datenschutzaufsichtsbehörde CNIL, zitiert nach Simitis (Simitis in: 2011, Einleitung, Rn. 220).

[1519] Siehe dazu Simitis (1997, S. 282 f., 287), der diesen Widerspruch zwar anspricht, aber offensichtlich nicht in der Lage ist, die Konsequenzen wahrzunehmen.

[1520] Simitis (1998, S. 2473).

[1521] Siehe Simitis (1998, S. 2478). Siehe auch die unterschiedlichen Formulierungen bei Simitis (1999, S. 5 f. und 18), die auf diese Gleichsetzung hinweisen.

[1522] So dann auch die deutlichere Trennung bei Sokol (1999, S. 3).

[1523] Siehe Simitis (1999, S. 29).

[1524] Siehe jeweils beispielhaft Rule und Brantley (1992), Belair et al. (1993), Sokol (2003), Vedder (1999) und Wright (1998).

[1525] Statt vieler siehe Roßnagel und Bizer (1995).

[1526] Siehe etwa Roßnagel (1997, S. 27 f.) oder Vesting (2003, 175 ff.). Zu den wenigen, die das Internet nicht als nur virtuellen Raum imaginieren, sondern die Notwendigkeit der Existenz von „physikalischen Pfeiler[n]“ und die

Dennoch werden daraus kühne Forderungen abgeleitet, vor allem zur Technikgestaltung und zum Technikeinsatz.[1527] Vor allem jedoch beginnt mit der Diskussion über Internet-bezogene Gefahren für *privacy* und Datenschutz eine Entwicklung zu einer zunehmenden Verengung der Perspektive: Während in der sonst durchaus vergleichbaren Debatte über „offene“ Netze in den 1980er Jahren noch die grundlegenden Eigenschaften offener Netze zum Gegenstand der Analyse gemacht wurde, verschiebt sich der Fokus der Debatte seit den 1990er Jahren immer mehr auf einzelne Teilaspekte und sogar einzelne Datenschnipsel – ob Cookies, Browserkennungen oder installierte Schriftarten. Auch kommt es zu einer extremen Zunahme an Wiederholungen in der Debatte, indem etwa alle *allgemeinen* Gefahren für *privacy* und Datenschutz, die im Zusammenhang mit dem System oder der Plattform S_1 diskutiert werden, nach dessen Ablösung durch das System oder die Plattform S_2 – und nachfolgend auch für S_3 bis S_n – als „neu“ diskutiert werden; so wird „Privacy bei Myspace“ einfach abgelöst durch „Privacy bei Facebook“. Und mit der zunehmenden Verbreitung des Internets werden auch nicht mehr – nur oder vorwiegend – Organisationen als Angreiferinnen betrachtet – wenn auch zumeist unter Rückgriff auf Theorien, die sich auf die Betrachtung interpersonaler Beziehungen beschränken –, sondern vermehrt auch Personen.[1528] Vor allem die Organisationen als Datenverarbeiterinnen profitieren von diesem Perspektivwechsel, die dadurch im Diskurs unsichtbar werden oder sich gar – in Verdrehung der realen Interessenkonstellationen und Machtverhältnisse – als „privacy guardians“ ihrer Nutzerinnen gerieren können.

Während die Kommodifizierung individueller Aktivitäten im Internet in der Debatte relativ breit problematisiert wurde,[1529] bleibt die Kommodifizierung sozialer Beziehungen im Netz lange Zeit eher unbeachtet.[1530]

2.5.2 Zum Verhältnis von Technik und Recht, oder: Zum falschen Traum von „code is law“

Die Debatte zum Verhältnis von Technik und Recht im *privacy*- und Datenschutzbereich und dazu, ob, inwieweit und in welcher Art und Weise rechtliche Anforderungen in informationstechnischen Systemen und Informationsverarbeitungsprozessen und mit Hilfe welcher Regelungsregime umgesetzt werden können, oszilliert zwischen zwei Polen: einerseits dem Verhältnis von Technik und Recht im Allgemeinen oder Abtrakten – unter anderem mit dem falschen, aber vielzitierten „code is law“ (Larry Lessig) – und andererseits dem Verhältnis von konkreten *privacy*- und datenschutzrechtlichen Regelungen zur Technik.[1531] Von dieser stark juristisch dominierten Debatte getrennt werden in einem vorwiegend informatisch geprägten Umfeld konkrete technische Ansätze sowie Analyse- und Entwicklungsmethoden diskutiert – von „Privacy Impact Assess-

daraus folgende Möglichkeit eines rechtlichen und rechtspraktischen Zugriffs verstehen – und zugleich darauf verweisen, dass die Anbieterinnen rechtlich greifbar sind –, gehört Dix (2000, S. 93).

[1527] Siehe etwa Hughes (1993) und Lutterbeck (2000). Besonders extrem in dieser Richtung und ohne irgendeine Begründung Federrath und Pfitzmann (2001, S. 1): „Der Betroffene kann und darf sich nicht mehr allein darauf verlassen, dass der Staat oder die speichernde und verarbeitende Stelle genügend unternehmen werden, um den Betroffenen zu schützen.“

[1528] Einer der Gründe dafür liegt wohl in der damals weitverbreiteten Annahme, dass das Internet als großer Gleichmacher wirke und sich zu einem Global Village entwickle. Es ist nicht übertrieben, diese „Visionen“ als „typische Phantasmen der 90iger Jahre“ (Hellige (2015)) zu bezeichnen, vielleicht sogar als *die* typischen Phantasmen.

[1529] Siehe etwa Simitis (1998, S. 2476 f., 2477) oder Weichert (2000).

[1530] Eine wichtige Ausnahme ist humdog (1994).

[1531] Siehe zur Übersicht mit einer extremen Beschränkung auf die englischsprachige Debatte Bennett und Raab (2003, S. 159 ff.).

ment“ über „Privacy by Design“ bis hin zu „Sticky Policies“ –, deren Verhältnis zum Recht oft unbestimmt bleibt und die dennoch nicht selten als „silver bullets“ verkauft werden.

Dabei fällt schon zu Beginn auf, dass die Beteiligten dieser Debatte in den 1990ern ihre Erkenntnis, dass Technik das Verhalten ihrer Anwenderinnen regeln würde, für eine neue Erkenntnis halten.[1532] Weitverbreitet ist auch ein sehr beschränktes Verständnis der jeweiligen gesellschaftlichen Probleme, etwa des *privacy*-Problems,[1533] in der Art, dass sie durch die jeweils ziemlich banalen technischen Mechanismen, die als Beispiele angeführt werden, gelöst werden können.[1534] Hinzu kommt ein sehr oberflächliches Verständnis von Technik, indem etwa behauptet wird, *das Netzwerk* könne Eigenschaften garantieren, die in der Realität jedoch technisch ausschließlich in den Endgeräten umgesetzt werden,[1535] oder es werden der Technik Eigenschaften unterstellt, die sie nicht hat.[1536] Damit zerfällt jedoch auch das zentrale Argument, nach dem „Lex Informatica“ „automated and self-executing rule enforcement“ erlaube[1537] – was immer Technik *durchsetzen* könne, sie kann sich nicht selbst *einsetzen* und in den meisten

[1532] Siehe Reidenberg (1998, S. 554, Fn. 5). Eine der zentralen Konsequenzen, die daraus gezogen wird – „code is law“ – ist dabei allerdings Humbug, insbesondere in der Form, die sie bei Lessig annimmt: „Architecture is a kind of law: it determines what people can and cannot do“ Lessig (1999, S. 59). Erstens ist es Humbug, weil Recht nicht festlegt, was Menschen – eigentlich: soziale Akteurinnen – tun oder nicht tun *können*, sondern nur, was sie *dürfen*. Zweitens ist auf der „code“-Seite nicht „code“ das Äquivalent zu „law“, sondern Anforderungen, Standards und Normen. Auch sie sind klassisch normativ und besitzen gleiche – oder zumindest sehr ähnliche – Eigenschaften wie Recht: Sie können unklar sein oder in sich widersprüchlich, Regelungslücken enthalten – siehe das Problem des „dangling else“ in C – oder miteinander in Regelungskonkurrenz stehen. Im Gegensatz zum gesellschaftlichen Bereich des Rechts gibt es jedoch im Technikbereich keine als allgemein legitim anerkannten Auslegungs- und Letztentscheidungsinstanzen. Die berühmte Normativität des Faktischen, die für die Technik unzweifelhaft gilt, stellt damit allerdings Technik zugleich auf eine Ebene mit „Organisation“ in dem Sinne, als Organisationen Recht – oder allgemeiner: Normen – *implementieren oder gerade nicht implementieren*, und anschließend die Organisation selbst zum begrenzenden Faktor der implementierten Norm wird, oder: Die Norm gilt nur noch insoweit, als sie von der Organisation umgesetzt wird, bzw. das, was die Organisation umsetzt, wird zur Norm. Siehe dazu auch Rotenberg (2001, Rn. 89). Und zumindest insofern hat Lessig dann wieder recht, wenn er schreibt: „control of code is power“ (S. 60), auch wenn er damit nicht über das hinausgeht, was zu diesem Zeitpunkt in der Debatte schon allgemein bekannt ist oder zumindest hätte sein sollen. In diese Richtung geht auch die Kritik Rotenbergs, siehe Rotenberg (2001, Rn. 17), der Lessig und seine Freundinnen der „kalifornischen Ideologie“ (Evgeny Morozov) als zu Recht „cyber pundits“ bezeichnet (Rn. 36). Und „code“ ist zugleich auch nicht, wie Lessig behaupt, direkt vergleichbar zu „physical architecture“ – oder wie Grimmelmann (2005, S. 1722) bemerkt: „You can hack a computer program into destroying itself; you will have no such luck hacking a highway.“

[1533] Siehe ganz grundlegend etwa Lessig (1999, S. 153 ff.), wonach Diskriminierung durch den Markt grundsätzlich gut sei.

[1534] Siehe etwa Reidenberg (1998, S. 560 ff., 569). Noch deutlicher wird dies bei Lessig: „a world where problems can be programmed away“, Lessig (1999, S. 13). Das zeigt sich auch daran, dass Lessig eine der zentralen sozialen Entitäten moderner Gesellschaften mit Missachtung straft: Organisationen. Siehe dazu seine Darstellung der Einflusskräfte Normen, Markt, Architektur und Recht, Lessig (1999, S. 88): Normen wirken „through the *stigma* that a *community* imposes“, Märkte durch Preise, Architekturen „throught the *physical* burdens they impose“ und Recht durch die Drohung mit Bestrafung – Organisationen kommen nicht vor, und die Gesellschaft ist eine Gemeinschaft!

[1535] Siehe etwa das HTTP-Beispiel bei Reidenberg (1998, S. 560).

[1536] Siehe die Ausführungen bei Lessig (1999, S. 27 ff.), wo die Eigenschaften als *absolute technische* Eigenschaften des Netzes beschrieben werden – „Net95 has no way to verify who someone is“ –, diese jedoch weder technisch ist, sondern sozial – die Technik ist da, aber wird nicht (oder nicht umfassend) eingesetzt –, und nicht absolut, sondern relativ *zu einem Zweck, der von der Verarbeiterin gesetzt wird*. Und wenn Lessig behauptet, dass „[u]nlike real space, cyberspace reveals no self-authenticating facts about identity“ wie Geschlecht, Alter oder Aussehen, sondern „only an address“ (S. 33), dann ist die Aussage falsch: In beiden Fällen wird alles aufgedeckt, was *innerhalb der Transaktion* liegt, und im Netz heißt das eben im Zweifelsfall auch: Web-Browser, Betriebssystem oder Herkunftsland. Siehe auch die Ausführungen zu TCP/IP bei Lessig (1999, S. 102).

[1537] Siehe Reidenberg (1998, S. 568).

Fällen ihren Einsatz gerade auch nicht erzwingen.[1538] Das komplette Fehlen einer Auseinandersetzung mit Organisationen und ihrem Technikgebrauch lässt darum auch sowohl Reidenberg wie Lessig übersehen, dass Recht Technikgebrauch steuern kann, ohne dies notwendig in Form einer Technikregulierung tun zu müssen.[1539] Noch schwerwiegender jedoch ist der Mangel an einer Auseinandersetzung mit den offensichtlichen Problemen, etwa wenn zur Norm wird, was in Technik umgesetzt wird, *indem es in Technik umgesetzt wird*, jedoch dabei die Rechte der Betroffenen beschnitten werden.[1540]

Auch die stark juristisch geprägte Diskussion zum Einfluss des Datenschutzrechts auf die Technik wie auch auf ihre Gestaltung nimmt immer wieder Bezug auf konkrete technische Systeme, ohne dass darüber reflektiert wird, in welchem Verhältnis das von der Technik „gelöste“ Problem zu dem Problem steht, das das Recht zu lösen versucht.[1541] So überrascht es kaum, dass Konflikte zwischen den Interessen der Datenverarbeiterinnen und denen der Betroffenen in einer Form als ausbalancierbar betrachtet werden, die die Grundentscheidung des Datenschutzrechts, den Schutz der Betroffenen in den Vordergrund zu stellen, strukturell unterminiert,[1542] ohne dass die Rechtswissenschaft darauf reagiert.

Einer der Pfeiler dieses neuen Verhältnisses zwischen Datenschutzrecht und Technik ist die Forderung nach einem „technischen Selbstschutz“, der – zusammen mit einer Selbstregulierung der Datenverarbeiterinnen – an die Stelle einer rechtlichen Regulierung der Datenverarbeitung durch verantwortliche Stellen treten soll.[1543] Dieser technische Selbstschutz, der auch als „Selbstdatenschutz“ bezeichnet wird, legt die Verantwortung für den Grundrechtsschutz in die Hand der

[1538] Daher bleibt es am Ende dann doch wieder dem Recht zugewiesen, für Entwicklung und Einsatz solcher technischer Systeme zu sorgen, siehe Reidenberg (2001, S. 9 f.), wenn auch ziemlich sicher ohne Kenntnis über vergangene Versuche in dieser Richtung. Siehe dazu auch die Kritik Rotenbergs an Lessig, in der er unter anderem darauf hinweist, „[t]he history of privacy protection is the history of the effort to regulate the design of technology (»code«) by means of public institutions“, Rotenberg (2001, Rn. 15).

[1539] Siehe Rotenbergs sarkastische Bemerkung „[t]here are no references in the Privacy Act to »PDP 11/70s«, »VAX 350s« or »Winchester (3030)« disk drives“, Rotenberg (2001, Rn. 42).

[1540] Siehe Podlech (1982, S. 460 f.) zum Gebot der Sicherung der Rechtsposition der Betroffenen als Teil des Systemdatenschutzes.

[1541] Ein geradezu klassisches Beispiel dafür ist der Beitrag von Cranor (2000b), in dem die Autorin sehr deutlich ausführt, gegen welche Gefährdungen die von ihr vorgestellten Werkzeuge schützen sollen, und der Umgang – oder besser: Nicht-Umgang – damit in allen anderen Beiträgen in diesem Band, vor allem denen von Juristinnen: Das Verhältnis zwischen den von Cranor adressierten Gefährdungen und sowohl dem Datenschutzproblem wie dem Datenschutzrechtsproblem wird einfach nicht bestimmt. Es wundert darum auch nicht, dass es keinerlei Auseinandersetzung zum Umgang mit der Differenz gibt, also der Menge an Problemen, die von der Theorie und vom Recht adressiert, von der Technik jedoch nicht gelöst wird.

[1542] Siehe etwa Rannenberg (1998, S. 193), wonach die Betroffenenrechte ebenso wie die Anforderungen aller anderen Parteien „Berücksichtigung“ finden müssten.

[1543] So etwa einer der Beschlüsse des 62. Deutschen Juristentages in Bremen 1998, siehe Deutscher Bundestag, Drucksache 14/850 vom 04.05.1999, Anlage 5. Siehe zur Diskussion auf dem DJT auch die etwas zugespitzte Darstellung bei Duttge (1998, S. 38 ff.). Auf die Untauglichkeit der Selbstregulierung als Regelungsinstrument wiesen schon damals Studien hin, siehe etwa Culnan (2000) mit einer Übersicht. Daran hat sich bis heute nichts geändert, siehe dazu Swire (2012). Das Grundproblem liegt dabei schon in der grundlegenden Problemdefinition, wie etwa Kloepfer (1998, S. 23) zeigt: Die Risiken werden als „Risiken der Informationstechnologien“ beschrieben. Siehe dazu auch die Ausführungen auf S. 66 ff., in denen die Verarbeitung personenbezogener Informationen als geradezu zwingend beschrieben wird, in denen von der extremen Ausdehnung organisierter Informationsverarbeitung gesprochen und gleichzeitig suggeriert wird, die Bedrohung gehe jetzt von „[N]achbar[n]“ aus, und in denen es nur um den Schutz von Daten und den Schutz vor „Einblicke[n] in die Privatsphäre“ geht – kein Wort zur Gefahr einer der Erhaltung und Ausdehnung der Handlungsspielräume entgegengesetzten Vorstrukturierung menschlichen Handelns durch übermächtige Organisationen, deren Machterhalt und Machtposition durch den Technikeinsatz sichergestellt und erweitert zu werden droht. Siehe dazu etwa Lenk (1982).

Betroffenen[1544] und entspricht damit durchaus dem neoliberalen Gesellschaftsverständnis.[1545] Damit einher geht eine mindestens teilweise Neudefinition der Rolle der Datenschutzaufsichtsbehörden: Zwar sollen sie noch immer Aufsicht über Datenverarbeiterinnen ausüben, wenn auch durchaus eher als Mitgestalterinnen von Technik und nicht nur zu deren nachträglicher Kontrolle,[1546] zugleich aber solle sich der Schwerpunkt ihrer Arbeit auf die Überzeugung der Betroffenen von der Notwendigkeit eines Selbstschutzes verschieben.[1547] Diese Reorientierung der Datenschutzaufsicht erinnert fatal an eine Krankenhausaufsicht, als deren Aufgabe definiert wird, den Patientinnen zu kommunizieren „Werdet nicht krank!“[1548]

Zur Frage, wie das Recht gestaltet werden müsse, um erfolgreich auf die Gestaltung der Technik Einfluss nehmen zu können, wird von der juristischen Debatte wenig Neues vorgelegt. Stattdessen wird vor allem auf bereits bestehende Gestaltungsansätze rekurriert, etwa den von *provet* vorgestellten, während sich beim Recht auf die allgemeinen Gestaltungsvorgaben verlassen wird.[1549] Und während große Einigkeit darüber besteht, *dass* Datenschutzbeauftragte Einfluss auf die Technikgestaltung nehmen sollen, bleibt die Debatte um die Frage des *Wie* ausgesprochen wolkig: Datenschutzbeauftragte sollen Entwicklerinnen „unterstützen“, etwa durch „Vorschläge für Standardkonfigurationen“,[1550] indem Entwicklerinnen „ihre Konzepte und Vorstellungen über Detaillösungen“ den Datenschutzbeauftragten zur Diskussion stellen und von diesen „Hinweise und Empfehlungen zur datenschutzgerechten Gestaltung“ bekommen[1551] oder durch „»projektbezogene Dreiecke« zwischen Herstellern und Anbietern aus der Wirtschaft einerseits, dem institutionalisierten Datenschutz andererseits sowie drittens der Wissenschaft“.[1552]

[1544] Siehe etwa Schrader (1998), Federrath und Berthold (2000), Roessler (2000).

[1545] Aus Informatiksicht liegt die zentrale Schwäche der Auseinandersetzung mit Selbstdatenschutzsystemen im Fehlen einer sauberen Trennung zwischen solchen technischen Systemen, die von Datenverarbeiterinnen kontrolliert werden und damit ausschließlich zu deren Bedingungen eingesetzt werden können, und solchen, die auch gegen den Willen der Datenverarbeiterinnen eingesetzt werden können. Während das grundsätzliche Problem in anderen Disziplinen zumindest angesprochen wird, siehe etwa schon Marcuse (1970) und Winner (1980), führt die Ignoranz der Informatik gegenüber diesem Problem zur strukturellen Unfähigkeit, die in die jeweiligen Informatiksysteme hineinkonstruierten Eigenschaften zum Gegenstand machen zu können. In einer etwas beschränkten Form findet sich eine diesbezügliche Regelung in § 26 des bündnisgrünen Entwurfes eines Bundesdatenschutzgesetzes von 1997, siehe Such und Fraktion Bündnis 90/Die Grünen (1997, S. 10).

[1546] Siehe etwa Federrath und Pfitzmann (1998) und Kessel (1998) zum Mitgestaltungsansatz, Roßnagel (1998) und Roßnagel (1999) zur Auseinandersetzung zum Datenschutzaudit sowie Klug (2001) zur Vorabkontrolle durch interne Datenschutzbeauftragte.

[1547] Siehe etwa Weichert (1998).

[1548] Siehe insofern die Ablehnung eines Einsatzes von Datenschutzbeauftragten als „vertrauenswürdige Dritte“ mit der Begründung, eine solche Dienstleistung würde mit ihrer Unabhängigkeit kollidieren, Fox (1998, S. 91). Das gilt sicher für die Unabhängigkeit der Datenschutzbeauftragten von den Datenverarbeiterinnen – gegenüber den Betroffenen würde es hingegen die Frage aufwerfen, ob die Datenschutzbeauftragten noch auf deren Seite stünden. Hingegen sehen Federrath und Pfitzmann (1998, S. 171 f.) gerade kein Problem in einer solchen Aufgabenzuweisung.

[1549] Siehe etwa Bizer (1998, S. 54 ff.), der diese Vorgaben als „relativ konkrete Vorgaben für die Gestaltung von [...]Techniken“ (S. 62) bezeichnet, obwohl sie weder konkret sind – „[d]ie Gestaltung und Auswahl technischer Einrichtungen [...] hat sich an dem Ziel, keine oder so wenige personenbezogene Daten wie möglich, zu verarbeiten und zu nutzen, auszurichten“ (§ 3 Abs. 4 Teledienstedatenschutzgesetz) – noch verpflichtend. Während Bizer (1999, S. 49 ff.) von einer Verpflichtung ausgeht – auch wenn er etwa in Bezug auf die EG-Datenschutzrichtlinie in diesem Zusammenhang nur auf Erwägungsgründe verweist (S. 53) –, hat sich die Regelung letztendlich als eben nicht verpflichtend erwiesen, siehe Pohle (2015a).

[1550] Siehe Federrath und Pfitzmann (1998, S. 170).

[1551] Siehe Kessel (1998, S. 182).

[1552] Siehe Bizer (1999, S. 59). Ein solches Modell wurde umfassend bislang ausschließlich beim Unabhängigen Landeszentrum für Datenschutz (ULD) Schleswig-Holstein institutionalisiert.

2.5.3 Modernisierung des Datenschutzrechts

Die EG-Datenschutzrichtlinie soll nach Art. 1 Abs. 1 „den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“ gewährleisten. Sie geht damit in ihrer Zieldefinition, wenn auch nicht in der Umsetzung in den konkreten Regelungen, von einem relativ breiten Verständnis von Datenschutz aus.[1553] Im Gegensatz dazu beschränkt sich das Bundesdatenschutz seit 1990 nach § 1 Abs. 1 darauf, „den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“

Im Zuge der Debatte um die Umsetzung der europäischen Vorgaben in nationales Recht und der allgemeinen Modernisierung des deutschen Datenschutzrechts wird eine Vielzahl an Regelungsansätzen und -mechanismen diskutiert – eine Wiederbelebung veralteter Konzepte wie der Sphärentheorie,[1554] die Forderung nach Rehabilitation der Generalklauseln[1555] und andererseits ihrer Ablösung[1556] oder die Forderung nach einer Abschaffung vieler formaler Pflichten der Datenverarbeiterinnen, etwa die Aufklärungs- und Unterrichtungspflichten, unter anderem wegen der „Papier- und Portoverschwendung“.[1557] Die Uninformiertheit der Debatte zeigt sich jedoch nicht nur im Verweis auf das „Porto-Problem“, sondern vor allem auch in der Fehlanalyse technischer und gesellschaftlicher Verhältnisse. Thilo Weichert glaubt, „[i]n Netzen, etwa im Internet, [seien] alle gleich“,[1558] für Bull ist es „schwer vorstellbar, wie [ein Geheimdienst] ohne gezielte, für den besonderen Zweck organisierte Informationssuche an wirklich relevante Persönlichkeitsdaten herankommen soll“, denn „sehr persönliche Lebensumstände“ gebe „niemand in einen Computer oder das Internet ein“,[1559] und Wolfgang Hoffmann-Riem glaubt, dass „Vorkehrungen zur sparsamen Datenerhebung“ „Elemente eines Selbstschutzes“ seien.[1560] Und wenn Christoph Gusy dem Datenschutzrecht das Paradigma eines „Schutz[es] vor Kommunikation“ unterstellt und dem das Ziel eines „Schutz[es] der Kommunikation“ gegenüberstellt,[1561] dann ist das nicht nur historisch falsch, denn Datenschutzrecht dient Schutz *in* der Kommunikation, sondern markiert zugleich eine Umdefinition der Angreiferin: Im Falle eines Schutzes *vor* oder *in* Kommunikation wird (mindestens auch) die Kommunikationspartnerin als Angreifern identifiziert, im Falle eines Schutzes *der* Kommunikation wird die Angreiferin als Außenstehende verortet, womit jedoch in vermachteten Verhältnissen die Angreiferinnenposition der Organisation einfach wegdefiniert wird.

Nachdem Anfang 2001 unter großem Zeitdruck vor dem Hintergrund eines von der EG-Kommission eingeleiteten Vertragsverletzungsverfahrens wegen der verspäteten Umsetzung der EG-Datenschutzrichtlinie in nationales Recht ein neues Bundesdatenschutzgesetz beschlossen wurde und in Kraft trat, das jedoch der erklärten Intention des Gesetzgebers nach so bald wie möglich grundlegend modernisiert werden sollte,[1562] wird diese Intention im wenig später publi-

[1553] Das ist eine der „zwei Säulen des Datenschutzes“ der Datenschutztheorie der 1970er Jahre bei Steinmüller et al. (1971, S. 60).

[1554] Siehe etwa Hoffmann-Riem (1998, S. 20, Fn. 25) oder noch extremer Petersen (2000, S. 148 f.), die wenig überraschend bei Bull promoviert hat.

[1555] Siehe etwa Bull (1998a, S. 32 f.), der allerdings zugleich fordert, dass der Gesetzgeber „ein *Verfahren* schafft, in dem die Interessengegensätze verarbeitet und ausgeglichen werden können.“

[1556] Siehe etwa Weichert (1999, S. 88 f.).

[1557] Siehe Bull (1998b, S. 314).

[1558] Siehe Weichert (1999, S. 86).

[1559] Siehe Bull (1998a, S. 27 f.).

[1560] Siehe Hoffmann-Riem (1998, S. 23).

[1561] Siehe Gusy (2000, S. 58).

[1562] Siehe dazu Simitis (Simitis in: 2011, Einleitung, Rn. 89 ff.).

zierten Gutachten von Roßnagel, Pfitzmann und Garstka im Auftrag des Bundesministeriums des Innern, „Modernisierung des Datenschutzrechts“,[1563] aufgegriffen.[1564]

Das Grundproblem des Gutachtens aus Sicht einer wissenschaftlichen Beschäftigung mit der historischen Konstruktion des Datenschutzes ist, dass im Gutachten zwar allenthalben exzessiv Kritik sowohl am konzeptuellen Ansatz der Abbildung des Datenschutzes im Recht wie auch an der konkreten Umsetzung geübt wird,[1565] die Autoren aber an keiner Stelle auf Literatur verweisen, aus denen sich ihre jeweiligen Zuschreibungen begründen ließen, kurz: Die von den Autoren als dem Datenschutzrechtsansatz zugrunde liegend behaupteten Vorstellungen, Annahmen und Grundentscheidungen sind schlicht nicht wissenschaftlich belegt. Das überrascht nicht. So behaupten die Autoren gleich zu Beginn etwa:

> „Das Datenschutzrecht ist vom Ansatz her orientiert an einer Datei personenbezogener Daten, die von einer verantwortlichen Stelle in einer zentralen Datenverarbeitungsanlage verarbeitet oder zu einer solchen übermittelt wird. Dieses Schutzkonzept ist in den 70er Jahren am Paradigma zentraler staatlicher Großrechner entwickelt worden, zwischen denen ein Datenaustausch die Ausnahme war.“[1566]

Was die Autoren als zugrunde gelegte Annahmen des Datenschutzrechts ansehen, sind in Wirklichkeit normative Vorgaben. Das gilt sowohl für den Begriff der „Datei“, mit dem der Geltungsbereich des Gesetzes eingeschränkt werden sollte, wie für den „*closed-shop*-Betrieb“.[1567] Auch wurde nicht die Existenz einer „zentralen Datenverarbeitungsanlage“ unterstellt oder angenommen, sondern der „Informationstechnologie“ wurde schlicht ein „instrumentaler Charakter“ unterstellt, der zugleich zur Annahme wie zur normativen Forderung führte, die Organisation werde und müsse dafür sorgen, dass sie die Technik unter Kontrolle habe.[1568] Und ob der Datenaustausch in der Praxis die Ausnahme war, darf erstens bezweifelt werden, ist zweitens jedoch auch irrelevant, denn gerade der Datenaustausch zwischen den – „vermaschten“ oder „integrierten“ – Systemen wurde als in naher Zukunft liegendes Problem adressiert.[1569]

An dieser auf Fehlannahmen basierenden Re-Konstruktion des Datenschutzrechts wird dann eine konzeptionell ebenso unsaubere Kritik geübt: Während die Autoren die konzeptionell saubere – und zugleich schon immer praktisch schwer zu trennende – Trennung zwischen der dem Gesetz unterworfenen und der nicht dem Anwendungsbreich unterfallenden Datenverarbeitung[1570]

[1563] Roßnagel et al. (2001).

[1564] Kai von Lewinski weist zu Recht auf den unglücklichen Zeitpunkt der Übergabe an das BMI, nämlich kurz vor den Anschlägen des 11. September 2001, hin, siehe von Lewinski (2014, S. 29, Rn. 63). Auf die Frage, inwieweit das Gutachten die von Lewinski beobachtete Zuschreibung einer „verpasste[n] Chance“ auch dann erhalten hätte, wenn es nicht gesetzgeberisch folgenlos geblieben wäre, sondern im Zuge eines umfassenden Gesetzgebungsprozesses ausführlich analysiert und kritisiert worden wäre, kann hier aus Platzgründen leider nicht eingegangen werden.

[1565] Siehe Roßnagel et al. (2001, S. 22 ff.).

[1566] Roßnagel et al. (2001, S. 22).

[1567] Siehe dazu jeweils Simitis (Simitis in: 2011, Einleitung, Rn. 219) und Steinmüller (1993, S. 675).

[1568] Siehe dazu Steinmüller (1976c, S. 10 f.) und Steinmüller (1993, S. 287).

[1569] Siehe zum praktisch stattfindenden Datenaustausch umfassend Steinmüller (1979a), zur Problematisierung etwa Kamlah (1970, S. 364), Steinmüller (1971c, S. 82), Podlech (1973b, S. 7 f.), Steinmüller (1975b, S. 49).

[1570] Die Trennlinie ist mit der Zeit immer wieder neu gefasst worden. Im BDSG 1977 war nur definiert, wer unter das Gesetz fällt: wer personenbezogene Informationen „für eigene Zwecke“ (§ 1 Abs. 2 Nr. 2) oder „geschäftsmäßig für fremde Zwecke“ (§ 1 Abs. 2 Nr. 3) „in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt“; das gleich galt für das BDSG 1990, nach dem Normadressat war, wer „geschäftsmäßig oder für berufliche oder gewerbliche Zwecke“ (§ 1 Abs. 2 Nr. 3) personenbezogene Information verarbeitet oder nutzt. Im BDSG 2001 ist die Menge der Normadressaten hingegen als Differenz formuliert: es sind alle, „es sei denn,

begrüßen, kritisieren sie diese Trennung als überholt, „wenn private und geschäftsmäßige Datenverarbeitung in der konkreten Anwendung oft nicht mehr von außen zu unterscheiden sein werden“, liefern aber nur mit der Sache nichts zu tun zu habende Begründungen.[1571]

Ähnlich falsch sind die Behauptungen, in den 1970er Jahren sei „die staatliche Datenverarbeitung als Hauptbedrohung“ gesehen worden, „[e]rst jüngste Datenschutzgesetze haben die Erkenntnis aufgenommen, dass die Gewährleistung von Datenschutz Anforderungen an Datenverarbeitungssysteme erfordert“, oder „die Globalisierung der Datenverarbeitung“ setze „dem nationalen Datenschutzrecht Grenzen“.[1572] Auch der Verweis auf die Leistungssteigerungen der Technik sowie neuere technische Entwicklungen geht vollkommen fehl:[1573] Ein Großteil der angesprochenen Entwicklungen – Geschwindigkeits-, Speicherfähigkeits- und Komplexitätssteigerung, Scoring, Auswertungsmöglichkeiten, Profilbildung, Biometrie – ist nicht neu und wurde bereits Anfang der 1970er Jahre umfassend analysiert, wenn sie auch nicht in allen Fällen zu Regelungen im Datenschutzrecht geführt haben. Und dass die „Nutzungsmöglichkeit neuer Kommunikations- und Informationstechnik die Zweckbindung der Datenverarbeitungs“ gefährdet, war nie anders und einer der Gründe für die Forderung ihrer Aufnahme ins Gesetz,[1574] genauso wie die zunehmende Intransparenz von Technik und Informationsverarbeitung. Allein die Ausführungen zur Intransparenz und Widersprüchlichkeit des Datenschutzrechts scheinen nicht aus der Luft gegriffen zu sein.[1575]

Bei den von den Autoren vorgeschlagenen Lösungsansätzen handelt es sich um eine weitgehend arbiträre Mischung von „bewährten“ Ansätzen,[1576] deren Bewährtheit allerdings unglück-

---

die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten“ (§ 1 Abs. 2 Nr. 3). Alle diese Regelungen sind davon geprägt, den Kreis der Normadressaten zu beschränken. Die Frage ist nur, auf welchen Kreis von sozialen Akteurinnen die Unterwerfung unter das Datenschutz beschränkt werden sollte. Die Frage ist nicht leicht zu beantworten, denn sie ist von den Beteiligten nie explizit beantwortet worden. Es ist jedoch sehr wahrscheinlich, dass nur oder vor allem Organisationen (im soziologischen Sinne) gemeint waren, denn andernfalls wären Mitarbeiterinnen (Mitglieder im soziologischen Sinne) von „Stellen“, die unter das Datenschutzrecht fallen, nach allen drei Definitionen selbst auch wieder „Stellen“ im Sinne des Gesetzes – und das hat bisher noch niemand behauptet.

[1571] Siehe Roßnagel et al. (2001, S. 23). So ist völlig unklar, was das mit „de[m] mobile[n] Mitarbeiter“ zu tun hat, der alle privaten und beruflichen Informationen auf dem gleichen Gerät verarbeite. Noch wesentlich kruder sind die Ausführungen zu den „in interaktiven Medien“ angeblich stattfindenden „ständige[n] Rollenwechsel[n]“ der Mediennutzerinnen „zwischen Vermittler und Empfänger von Informationen“, die dann „zu einer ebenso genauen wie detaillierten Kenntnis ihrer Vorstellungen, Gewohnheiten und Erwartungen aus verschiedenen Lebensbereichen“ in der Hand von Datenverarbeiterinnen führen würden – mit einer Veränderung auf Seiten der Datenverarbeiterinnen hat dies allerdings nichts zu tun. Und gegenüber den Betroffenen ist der Vorwurf, die Freiheiten der neuen Kommunikationsmittel zu nutzen, ungefähr so angemessen wie ein Vorwurf gegenüber Vergewaltigungsopfern, sie würden sich zu aufreizend gekleidet haben.

[1572] Siehe Roßnagel et al. (2001, S. 23, 25, 26). Staatliche und private Datenmacht wurden, anders als die Autoren behaupten, als gleich gefährlich erachtet, siehe schon Lenk (1972, S. 5 f.): „To a large extend, this means that availability of person-related information considerably facilitates the exercise of power on individuals and thus increases this power. This concerns private power as well as the State [...].“ Genauso falsch ist, dass die Gestaltung der technischen Systeme ignoriert worden sei, siehe Pohle (2015a). Und die weltweite Anwendbarkeit und Anwendung des US-amerikanischen Einkommenssteuerrechts widerlegt die dritte Behauptung – es kommt auf die konkrete Umsetzung im Recht an, nicht darauf, ob es national ist. Daher ist auch, wie die EU-Datenschutzgrundverordnung zeigt, die Normierung des Marktortprinzips eine Lösung in einem nationalen oder regionalen Recht für ein globales Problem.

[1573] Siehe Roßnagel et al. (2001, S. 26 ff.).

[1574] Siehe zur Zweckbindung als zugleich normatives und kontrafaktisches Prinzip umfassend Pohle (2015b).

[1575] Siehe Roßnagel et al. (2001, S. 29 ff.).

[1576] Siehe dazu und zum folgenden Roßnagel et al. (2001, S. 35 ff.). Dazu gehört etwa ein extrem unterkomplex gedachtes „Recht auf informationelle Selbstbestimmung als Schutzgut“, siehe auch S. 46 ff., das seiner historischen funktionalistischen Konstruktion durch Steinmüller als Regelkreismodell für die Beeinflussung von Freiheits-

licherweise mangels Begründung nicht überprüfbar ist, und „neuen“ Konzepten wie Systemdatenschutz und Selbstdatenschutz, mit denen die identifizierten Ziele – „Datenschutz durch Technik“, Transparenz, Vermeidung des Personenbezugs, der Entwicklung von Betroffenen „zu Teilnehmern des Datenschutzes“ und der Einbettung des Datenschutzes in eine „Informations- und Kommunikationsordnung“ – durch „Anreize“ wie Auditierung, Zertifizierung oder „Erleichterung der rechtlichen Anforderungen“ etwa beim Einsatz „zertifizierter datenschutzfreundlicher Produkte“ erreicht werden sollen. Selbst offensichtliche Lücken in diesen Lösungsansätzen werden nicht problematisiert oder sollen mit dem gleichen Mechanismus gelöst werden, der vorher am bestehenden Recht kritisiert wurde, etwa wie ein weltweiter Einsatz datenschutzfreundlicher Technik sichergestellt werden soll, wenn er nur *national und rechtlich* erzwungen werden kann.[1577] Während auch diese Autoren nicht begründen, warum sie für das Datenschutzrecht eine Selbstbeschränkung auf personenbezogene Informationen vorsehen,[1578] präsentieren sie zumindest einen guten Vorschlag für den Ausgleich zwischen der allgemeinen Informationsfreiheit aus Art. 5 Abs. 1 Satz 1 GG und dem Datenschutzrecht: Personenbezogene Informationen „aus allgemein zugänglichen Quellen“ sollen datenschutzrechtlich nur für die Phasen der Erhebung und der Speicherung privilegiert werden, nicht jedoch für andere Phasen.[1579]

Besonders problematisch an dem Gutachten ist der Begriffsgebrauch, der auf eine beschränkte analytische Schärfe verweist und sich durch das gesamte Gutachten zieht: Die Autoren machen an keiner Stelle deutlich, ob sie über Informationsverarbeitung – durch soziale Akteurinnen – sprechen oder über Datenverarbeitung – durch technische Systeme. Aus dem Gutachten wird daher nicht deutlich, dass den Autoren der Unterschied sowie die Konsequenzen der Unterscheidung bewusst sind. Weil ihnen darüber hinaus ein umfassendes und zugleich in sich konsistentes Konzept zur Gefährdungsanalyse fehlt, verlieren sie sich in Detailregelungen, die sie wahllos aus ordnungs- und technikrechtlichen Ansätzen zusammenmischen, und deren spezifischen Begründungszusammenhängen. Und weil sie die Phasenorientierung weder als ein zu übernehmendes bisheriges Datenschutzkonzept identifizieren noch sonst im Gutachten reflektieren, kann ihnen auch gar nicht auffallen, dass die von ihnen an einigen Stellen ins Spiel gebrachten Schutzziele, die selbst aber auch nicht als methodischer Ansatz analysiert werden, die Frage aufwerfen müssten, ob, inwieweit und in welcher Form Phasen und Schutzziele kombiniert werden können und müssen, oder ob eine konsequente Schutzzielausrichtung des Datenschutzrechts eine grundsätzliche Alternative zur Phasenorientierung bieten könnte.

Zusammenfassend ist festzustellen, dass das Gutachten eine Fleißarbeit ist, in der viele der damals diskutierten Ansätze dargestellt und eingeordnet werden, jedoch kein großer Wurf im Hinblick auf eine notwendige Aktualisierung einer Analyse des Datenschutzproblems im beginnenden 21. Jahrhundert.

2.5.4 Die „neuen“ Theorien

Zwischen Mitte der 1990er und Anfang der 2000er Jahre wurde eine relativ große Menge an Werken publiziert, in denen die Autorinnen für sich in Anspruch nahmen, neue – oder zumindest grundlegend überarbeitete – *privacy-*, *surveillance-* oder Datenschutztheorien zu präsentieren oder diese konzeptionell neu zu ordnen.

räumen, siehe Steinmüller et al. (1971, S. 87), komplett entkleidet ist, und als reines Geheimschutzprinzip verstanden wird, siehe S. 40, Fn. 66.

[1577] Siehe Roßnagel et al. (2001, S. 35 und 40).

[1578] Siehe Roßnagel et al. (2001, S. 61 sowie 97 ff.).

[1579] Siehe Roßnagel et al. (2001, S. 62 f.).

In einer von Simitis betreuten Dissertation zur den Prinzipien und Zielen des Datenschutzes versucht Pelopidas Donos, mit einer Verbindung von Luhmannscher Systemtheorie und Habermas'scher Kommunikationstheorie, indem er als die Gesellschaft zugleich als System und als Lebenswelt betrachtet, den Datenschutz als Schutzgegenstand des Datenschutzrechts zu bestimmen.[1580] Wie bei Rüpke, den er auch zitiert, ist auch bei Donos die Hauptaufgabe des Datenschutzes „die Bewahrung der kommunikativen Integrität der Betroffenen“, also „die Gewährleistung einer autonomen Reproduktion der Lebenswelt der Betroffenen durch ungestörte kommunikative Handlungen“ gegen die „kommunikationsstörende Funktion von Datenverarbeitungssystemen, welche die Kommunikation entsprachlichen und die soziale Handlungskoordinierung beeinträchtigen können.“[1581] Damit will Donos sich von den als defensiv beschriebenen Datenschutztheorien abgrenzen, namentlich Rollentheorie und Systemdatenschutz, „welche die Aufgabe des Datenschutzes auf den Schutz oder Mitgestaltung der jeweiligen Datenrolle reduzieren“, und stattdessen „kommunikative Räume schaffen, in denen sich die individuellen Lebenswelten reproduzieren und die Personen sich kommunikativ entfalten können“ und zugleich der „substanzielle[n] Rolle des Datenschutzes bei der Formierung von autonomen Öffentlichkeiten“ dienen.[1582] Zugleich erklärt er aber die „Legitimation der Datenverarbeitung“ zur zentralen Aufgabe des Datenschutzes, indem es durch seine „Prozeduren“ dafür sorge, dass „jede Datenverarbeitung und jede Datenrolle [im Sinne eines Profils] in der Lebenswelt der Betroffenen diskursiv thematisiert werden.“[1583]

In einem Artikel, in dem er zugunsten einer Grundregel, die nur „functionally necessary“ Verarbeitung personenbezogener Informationen erlaubt, wenn nichts anderes vereinbart worden sei, eintritt – natürlich ohne auf die europäischen Vorarbeiten dazu zu verweisen –, ordnet Jerry Kang die ihm bekannten *privacy*-Konzepte drei Clustern zu: „space“, „decision“ und „information“ – einem physischen Raum, der vor dem Eindringen geschützt sein solle, der Freiheit, ohne Einmischung von außen Entscheidungen treffen zu können, sowie der Kontrolle der Betroffenen über die Verarbeitung personenbezogener Informationen.[1584]

Raab und Bennett argumentieren, dass es nicht ausreiche, bereichsspezifische Regelungen zur Datenverarbeitung zu erlassen, sondern in den jeweiligen Bereichen auch analysiert werden müsse, inwieweit verschiedene Gruppen von Betroffenen – Junge und Alte, Arme und Reiche, Gesunde und Kranke – unterschiedlichen Risiken in unterschiedlichem Umfang ausgesetzt seien, und das Recht darauf dann eine Antwort zu finden habe.[1585] Darüber hinaus müsse das Recht sich von einem rein prozeduralen Ansatz lösen und sich einem materiell-rechtlichen Ansatz nähern,

[1580] Siehe Donos (1998). Die Tatsache, dass er bei Simitis promoviert hat, zeigt sich etwa daran, dass er die „Erfindung“ der Phasenorientierung explizit Steinmüller und Lutterbeck abspricht, sondern sie ihnen als Argument gegen eine rein systemtheoretische Betrachtung des Datenschutzes vorhält, siehe S. 40. Und die Bezugnahme auf das HDSG legt nahe, dass er glaubt, Simitis habe die Phasenorientierung erfunden.

[1581] Siehe Donos (1998, S. 55, Fn. 152 und 54).

[1582] Siehe Donos (1998, S. 54 f.). Wie sich an Rost (2014a) sehen lässt, lässt sich die Reproduktion von Lebenswelten auch innerhalb der Theorie sozialer Systeme adressieren, nämlich als Personenkonzepte mit ihren Freiheits-, Autonomie- und Souveränitätsversprechen.

[1583] Siehe Donos (1998, S. 60).

[1584] Siehe Kang (1998, S. 1202 f.). Diese Einteilung, die selbst schon in einer Tradition sehr ähnlicher Einteilungen steht, zuerst wohl Conklin (1976), darauf aufbauend Burgoon (1982) und mit einigem Abstand DeCew (1997), wird später ohne Herkunftsangaben von Rössler (2001) übernommen und gewinnt nachfolgend einige Popularität in der *privacy*- und Privatheitsdebatte, vor allem in der deutschsprachigen, allerdings immer nur mit Verweis auf Rössler.

[1585] Siehe Raab und Bennett (1998).

auch um überprüfbar machen und überprüfen zu können, ob und inwieweit das Recht tatsächlich das betreffende Schutzgut schütze.[1586]

Paul Schwartz hingegen verfolgt – wenig überraschend, nachdem er Post-Doc bei Simitis war – einen klassisch europäischen Ansatz, indem er *privacy* als funktionale Voraussetzung für individuelle Selbstbestimmung und deliberative Demokratie markiert, wenn auch ohne anzugeben, von wo er diesen Ansatz übernommen hat.[1587] Diese würden, so Schwartz, durch das „managerial data processing model" rationaler Bürokratien im Weberschen Sinne, im Internet strukturell unterlaufen, weshalb *privacy* nur zu retten sei mit einem – nicht explizit so genannten – europäischen Regulierungsansatz: „(1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight", die weder durch den Markt noch durch Selbstregulierung geleistet werden könnten, sondern nur durch das Recht.[1588] Dieses Modell sei einem theoretisch wie praktisch unterkomplexen und von ihm als „privacy-control" bezeichneten „personal right to control the use of one's data"[1589] vorziehen, denn es gehe darum den Zugriff von Staat und Gemeinschaft auf personenbezogene Informationen zu beschränken „as a necessary means of restricting these entities' sovereignty" über die Normierung von Verhalten „to allow the necessary independence of social expression and action".[1590] Im Hintergrund steht eine an die frühe Datenschutzdebatte erinnernde Analyse der individuellen und gesellschaftlichen Folgen von Informationsmacht, bei der „the structure of access to personal information can have a decisive impact on the extent to which certain actions or expressions of identity are encouraged or discouraged."[1591]

In diese von Paul Schwartz und William Treanor als „new privacy" bezeichnete Strömung gehören auch die Arbeiten von Priscilla Regan, Julie Cohen und Daniel Solove, die dort ansetzen würden, wo die Annahmen der „old privacy", die auf „shared, pre-existing norms of the private" basierten, unzureichend seien, weil sie die Realitäten des „modern bureaucratic state" nicht entsprächen.[1592] Im Gegensatz zu Schwartz verweist Cohen im Jahre 2000 zumindest darauf, dass die Autorinnen der EG-Datenschutzrichtlinie „agreed with [Cohen's] characterization", wonach Informationsverarbeitungen verhindert werden sollten, „that threat individuals as mere conglomerations of transactional data, or that rank people as prospective customers, tenants, neighbors, employees, or insureds based on their financial or genetic desirability", um die Autonomie der Betroffenen als „an essential independence of critical faculty and an imperviousness to influence" in einer „zone of relative insulation from outside scrutiny and interference" – oder in Rückgriff auf Goffman: „a field of operation within which to engage in the conscious construction of self" – zu sichern; kurz: es gehe um den Schutz der „boundaries that insulate different spheres of behavior from one another."[1593] Gleichwohl wird auch bei Cohen dieser Autonomiebereich nicht

[1586] Siehe dazu auch Raab und Bennett (1996).

[1587] Siehe Schwartz (1999b).

[1588] So seine Schlussfolgerung Schwartz (1999b, S. 1701). Seine zwei zentralen Grundsätze sind das Erforderlichkeitsprinzip und das Zweckbindungsprinzip, siehe S. 1674.

[1589] Siehe Schwartz (1999a, S. 820).

[1590] Siehe Schwartz (1999a, S. 843).

[1591] Siehe Schwartz (1999a, S. 834). Zumindest etwas wird diese Verbindung später expliziert, wenn auch nur am Rande, siehe Schwartz (2003, S. 2101 und 2115 f.), wo er zugleich ein „property model" konstruiert und fünf Anforderungen statuiert, die an einen Markt für personenbezogene Informationen zum Schutz von „individual privacy" und „democratic order" zu stellen seien.

[1592] Siehe Schwartz und Treanor (2003, S. 2179). Vor dem Hintergrund, dass zumindest Schwartz es besser weiß, ist sowohl die Bezeichnung als „new privacy" wie auch die Auswahl der Autorinnen mehr als fragwürdig, aber sie alle werden in der *privacy*-Debatte breit rezipiert.

[1593] Siehe Cohen (2000a, S. 1424 f.). Das ist alles auch nicht neu, aber zumindest gibt Cohen an, auf wen sie sich dabei stützt, unter anderem Goffman, Westin, Post und Allen, S. 1423 ff. Auf die EG-Datenschutzrichtlinie

bedroht, wenn es nur darum gehe, „knowledge about groups“ zu erheben und zu verarbeiten.[1594] An Goffmans auf interpersonale Beziehungen beschränkten Theorie hält Cohen auch später fest – und nimmt gleich noch Altman hinzu –, wenn sie mit den Surveillance-Studies-Theorien versucht, die Bedingungen, unter denen Menschen und ihr Verhalten transparent gemacht werden können und werden, und die Kontrolle über diese Bedingungen zu problematisieren,[1595] um am Ende ganz bei Altmans „boundary management“ und ähnlichen sozialpsychologischen Ansätzen zu landen, denen noch Reste von postmodernen Theorien zur „self-formation“ zur Seite gestellt werden.[1596]

Auch Soloves Arbeiten zeigen viele Parallelen zur Datenschutzdebatte der 70er und 80er Jahre, etwa indem er auf der Basis von Webers Bürokratieverständnis die gleichen Folgen moderner Informationsverarbeitung für Individuen und Gesellschaft identifiziert, die schon das BVerfG im Volkszählungsurteil problematisierte, und deshalb argumentiert, dass nicht Orwells „1984“, sondern Kafkas „Der Process“ die angemessenere Metapher für sein *privacy*-Problem sei.[1597] Auf der Basis von Wittgensteins Konzept der Familienähnlichkeit versucht er sich dann „on understanding privacy in specific contextual situations“, kommt dabei allerdings nicht darüber hinaus, die von ihm untersuchten sozialen Praktiken – sowohl deskriptiv wie normativ – in das Schema von „private“ vs. „not private“ zu pressen, um dann den Wert von *privacy* instrumental anhand des Kontextes bestimmen zu wollen.[1598] 2006 schließlich legt Solove eine Taxonomie der *privacy*-Verletzung vor, die „the activities that invade privacy“, die er identifiziert, in vier Gruppen einteilt: „(1) information collection, (2) information processing, (3) information dissemination, and (4) invasion“, wobei es sich nicht um *privacy*-Verletzungen handeln solle, wenn die Betroffene einwillige.[1599] Im Gegensatz zu seinen vorhergehenden Arbeiten beschränkt er sich bei der Angreiferin nicht mehr auf bürokratische Organisationen, sondern betrachtet „various entities (other people, businesses, and the government)“.[1600] Weder für diese Entscheidung noch für die Auswahl der betrachteten Aktivitäten liefert er eine Begründung,[1601] und die konzeptionelle Verwandtschaft zum Gutachten „Grundfragen des Datenschutzes“ ist fast vollständig unbeachtet geblieben.[1602]

Auf der anderen Seite behauptet Amitai Etzioni, ein kommunitaristisches *privacy*-Konzept vorzulegen,[1603] präsentiert aber eigentlich nur eine hochgradig individualistische Konzeption des zugrunde liegenden Interesses, dem er dann seine Gemeinschaftsideologie entgegensetzt und diese

als Quelle verweist sie auch in ihrem Abschnitt „Informational Privacy in Practice“ (S. 1428 ff.) an mehreren Stellen.

[1594] Siehe Cohen (2000a, S. 1430).

[1595] Siehe dazu Cohen (2008).

[1596] Siehe Cohen (2013).

[1597] Siehe Solove (2001) und ausführlicher Solove (2004).

[1598] Siehe Solove (2002).

[1599] Siehe Solove (2006, S. 485, 488 und 484). Die einzelnen Aktivitäten sind dabei für Information Collection: Surveillance und Interrogation; für Information Processing: Aggregation, Identification, Insecurity, Secondary Use und Exclusion; für Information Dissemination: Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation und Distortion; für Invasion: Intrusion und Decisional Interference.

[1600] Siehe Solove (2006, S. 488). Überraschenderweise findet er in einer späteren Arbeit zu seiner auf bürokratische Organisationen eingeschränkten Analyse zurück, wenn er das „I've got nothing to hide“-Argument als Produkt eines sehr beschränkten *privacy*-Konzeptes entlarvt, in dem *privacy* für „hiding bad things“ steht, und mehr noch, sich konzeptionell nur auf „concealment or secrecy“ beziehen kann, siehe Solove (2007, S. 764).

[1601] Die Begründung folgt auch nicht in seinem umfassenden, seine Vorarbeiten zusammenfassenden Werk, siehe Solove (2009).

[1602] Siehe Pohle (2014a, S. 53 und 55, Endnote 4).

[1603] Siehe grundlegend Etzioni (1999a) und Etzioni (1999b).

als übergeordnet behauptet. *Privacy* ist dann am Ende bei ihm nichts anderes als „a *societal license* that exempts a category of acts (including thoughts and emotions) from communal, public, and governmental scrutiny“,[1604] wobei das ganz wesentlich das Ergebnis einer extrem verkürzten Darstellung in den vorangegangenen Kapiteln ist, wo er alle Auseinandersetzungen unterschlägt, die nicht in sein Trivial-Schema passen: die Datenverarbeiterinnen vertreten das „common good“ – selbst die privaten[1605] –, während die Betroffenen nur „individual rights“ dagegensetzen können.[1606] Während Etzioni einerseits behauptet, zwischen „social scrutiny“ und „governmental control“ zu unterscheiden,[1607] macht er andererseits immer wieder den Staat zum Sachwalter seiner – eher an eine Sekte erinnernde – Gemeinschaft, wobei es für Etzioni ausreicht, wenn der Staat sich auf ein „öffentliches Interesse“ beruft – er muss es nicht einmal begründen.[1608]

In eine sehr ähnliche Richtung geht Robert Posts Kritik an Jeffrey Rosens Konzept von *privacy* als Schutz vor einem „unwanted gaze“ – dem unerwünschten Starren –, vor einem „being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge“ aufgrund des Risikos zur Missinterpretation:[1609] Für Post ist die Fremddefinition des Menschen gerade das „Soziale“ und gleichzeitig das Effiziente, das Gute und das Wünschenswerte.[1610]

Diese Kontextgebundenheit hat noch viel stärker Helen Nissenbaum in den Fokus genommen, dort allerdings nicht nur im Sinne des Herkunftskontexts von Informationen, sondern auch im Sinne der Erwartungen der Betroffenen an den Verwendungskontext.[1611] Wie schon einige vor ihr hatte Nissenbaum festgestellt,[1612] dass eine Konzeption von *privacy* „all information, including information gathered in so-called public realms“ umfassen müsse, denn es gebe eine „multiplicity of contexts“ in dem Sinne, dass „[i]nformation learned in one context belongs in that context and is public vis-à-vis that context“, wofür sie dann behauptet, dass „[p]eople count on this contextual integrity as an effective protection of privacy“: „Privacy, in enabling individuals to

[1604] Etzioni (1999b, S. 196).

[1605] Siehe etwa Etzioni (1999b, S. 139 ff.), was wohl auch erklärt, warum er ein großer Fan von Selbstregulierung durch die „business community“ ist, siehe S. 160 ff.

[1606] Siehe auch die Kritik bei Schwartz (1999a, S. 838 ff.).

[1607] Siehe etwa Etzioni (1999b, S. 212 ff.).

[1608] Siehe dazu umfassend Etzioni (2015).

[1609] Siehe Rosen (2000b, S. 8), siehe auch Rosens Antworten auf einige der vorgebrachten Kritiken: Rosen (2000a) und Rosen (2001). Nichts an dem Konzept ist neu, auch und gerade nicht das Verhaftetbleiben an der Privat-öffentlich-Dichotomie, die sich durch alle seine Texte zieht. Siehe auch die Kritik von Cohen (2000b) an Rosens mangelhafter Ursachenanalyse, die ihm entgegenhält, es gehe nicht einfach um irgendeinen Moralismus, der anderen oktroyiert werde, sondern die „destruction of privacy is the necessary byproduct of a particular set of beliefs about the predictive power of information that operate in both market and government spheres“, siehe S. 2033.

[1610] Siehe Post (2000). Das liegt wohl auch an seinem abstrusen (Volks-)Gemeinschaftsbegriff, auf den gestützt er behauptet, der Schutz von Menschenwürde „seeks to eliminate differences by bringing all persons within the bounds of a single normalized community“, siehe S. 2095. Siehe auch die Kritik von Ehrenreich (2001), die unter anderem genau wegen dieser Frage von Selbst- und Fremddefinition nicht von „privacy“ sprechen will, sondern von „power“.

[1611] Siehe grundlegend Nissenbaum (2004) sowie umfassend Nissenbaum (2010), wo sie diese „privacy expectations“ dann „norms of information flow“ und „context-relative informational norms“ nennt, siehe S. 129 und 140. Siehe auch die Diskussion zur Überschneidung mit dem Prinzip der „reasonable expectations of privacy“ auf S. 233 ff.

[1612] Siehe Nissenbaum (1997) und Nissenbaum (1998) unter Verweis auf Rachels (1975) – wenn auch in der in Schoeman (1984a) abgedruckten Fassung –, einer vereinfachten Form der Analyse von Müller (1975a) und Müller (1975b). Zu den wenigen, die eine solche Verbindung sehen, gehören Holtz und Schallaböck (2011, S. 344), die Nissenbaums Ansatz mit Luhmanns funktionaler Differenzierung in Zusammenhang bringen.

maintain contextual integrity, enables them to develop a variety of distinct relationships.“[1613] Kontexte seien dabei „structured social settings characterized by canonical activities, roles relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)“ und können unterschiedlich granular sein, sich überschneiden und auch konfligieren, um dann ausgehandelt zu werden.[1614] In der Folge fasst sie „contextual integrity“ als Maß für die Erfüllung der „informational norms“.[1615] Akteurinnen – „senders of information, recipients of information, and information subjects“ – können „single individuals, multiple individuals, or even collectives such as organizations, committees, and so forth“ sein, aber gerade Organisationen werden hinsichtlich ihrer spezifischen Eigenschaften *als Organisationen* nicht adressiert, Informationen sind für sie das gleiche wie Daten im technischen Bereich, und in der Betrachtung beschränkt sie sich auf Informationsflüsse im engeren Sinne.[1616] Anschließend nutzt sie „contextual integrity“ als Framework zur Untersuchung von Veränderungen, die sich aus der Einführung neuer Technik oder dem Einsatz neuer Praktiken ergeben, die dann bewertet werden können und sollen.[1617] In ihrem abschließenden Kapitel wird deutlich, wie wenig Neues und wie wenig Potential ihr Ansatz birgt, wenn sie etwa feststellt, dass „contextual integrity“ im Grunde das gleiche sei wie die „reasonable expectation of privacy“, die amerikanische Gerichte seit der Katz-Entscheidung 1967[1618] verwenden, oder wenn sie in der Gegenüberstellung zwischen umfassender und sektoraler Regulierung nur an der Oberfläche bleibt und pauschal die sektorale vorzieht, indem sie nicht nur Mischformen aus allgemeinen und bereichsspezifischen Gesetzen wie in der Bundesrepublik ignoriert, sondern gerade auch die Auseinandersetzungen, die zu diesen Mischformen geführt haben.

[1613] Siehe Nissenbaum (1997, S. 215 f.). Nissenbaum verweist in ihrer Arbeit auf frühere *privacy*-Theoretikerinnen, ordnet deren Ansätze aber nicht in soziologische Theorien ein, die diesen Ansätzen zugrunde liegen, und offensichtlich haben sie auch weder die Peer-Reviewer noch die Leute, denen sie ihren Dank für Kommentare und Anregungen ausspricht, darauf hingewiesen, sonst hätte sie zumindest festgestellt, dass Schoeman (1992), den sie auch zitiert, siehe Nissenbaum (1998, S. 583, Fn. 57), mit seinen „spheres of life“ gerade das Setting adressiert, in dem Goffman oder Parsons ihre Konzepte von sozialer Rolle verorten und einbetten. Siehe dazu auch Hoffmann (1991, S. 127). Nissenbaum und Kolleginnen selbst sehen an anderer Stelle durchaus, dass dieser Ansatz nicht neu ist, aber anstatt eine Übernahme einzugestehen, umschreiben sie die Existenz der Vorarbeiten damit, dass die Idee einfach „in the air“ gewesen sei, siehe Barth et al. (2006, S. 2).

[1614] Nissenbaum (2010, S. 132 ff.).

[1615] Nissenbaum (2010, S. 140).

[1616] Nissenbaum (2010, S. 141 ff.). Während Nissenbaum selbst Kang, siehe Kang (1998), mit einem weiten Begriff von „control“ zitiert (S. 71), benutzt sie dann einen viel engeren, um zu „zeigen“, dass ihre Betrachtung von „transmission principles“ als „constraint[s] on the flow (distribution, dissemination, transmission) of information from party to party in a context“ (S. 145) umfassender sei, während er in Wirklichkeit noch enger als Kangs ist und weder „processing“ noch „use“ umfasst, aber auch nicht „deletion“. Sie bleibt damit weit hinter dem zurück, was etwa Müller schon Mitte der 1970er Jahre mit seinem Vorschlag für eine überlegte, nämlich funktions- und kompetenzorientierte Zuweisung von Informationen für das informationelle Handeln von Institutionen, die Gestaltung von Informationsflüssen und damit „Regelungen der »Informationshaushalte« von Institutionen oder Sektoren der Gesellschaft“ vorgelegt hatte, siehe Müller (1975a, S. 123).

[1617] Nissenbaum (2010, S. 148 ff.). Das ist problematisch, weil es ein „Vorher“ notwendig voraussetzt, anhand dessen Veränderungen nur untersucht werden können, und zugleich, weil damit nur Veränderungen – und sehr wahrscheinlich nur relativ abrupte und jedenfalls nur die sichtbaren –, dafür aber jede einzelne als „red flag“ (S. 150) markiert wird, siehe auch die Diskussion auf S. 159 ff., etwa auch die Einführung von E-Mail *per se*. Insofern ist ihre „Heuristik“ (S. 148) zugleich sowohl zu weit und nicht weit genug gehend. Siehe auch die Kritik bei Birnhack (2011, S. 70 ff.), der unter anderem darauf verweist, dass Nissenbaums Ansatz, den Status quo zur Referenz zu machen, „might legitimize and reinforce an unfair equilibrium achieved by a powerful party at the expense of relatively powerless other parties.“

[1618] Katz vs. United States, 389 U.S. 347 (1967).

Auf der Basis von Altmans Theorie von *privacy* als „boundary management“ werden zu Beginn des neuen Jahrtausends einige „neue“ *privacy*-Theorien publiziert, die allerdings alle nur auf interpersonale Beziehungen abzielen,[1619] und deren beschränkter Geltungsbereich nicht problematisiert wird:[1620] Weil nur interpersonale Beziehungen betrachtet werden, in denen die Akteurinnen als strukturell gleich mächtig angenommen werden, lässt sich einfach unterstellen, dass „revealing and concealing“ durch die Betroffene ausgehandelt werden könne – eine Unterstellung, die im Verhältnis gegenüber Google oder dem Staat einfach nur lächerlich ist.[1621]

Und auch die Surveillance Studies als eine „cross-disciplinary initiative to understand the rapidly increasing ways in which personal details are collected, stored, transmitted, checked, and used as means of influencing and managing people and populations“[1622] behaupten, dass sie sich weiter entwickeln müssten und würden, denn die „new surveillance“ sei anders als die „old surveillance“:

> „more intensive and extensive than previous forms and transcends distance, darkness, physical barriers and time; its records can be stored, retrieved, combined, analyzed and communicated with great ease; it has low visibility or is invisible; is often involuntary; emphasizes prevention; is capital rather than labor intensive; involves decentralized control and triggers a shift from targeting a specific individual to categorical suspicion.“[1623]

Dabei werden zumindest auch wieder alte, wenn auch schon beantwortete Fragen neu aufgeworfen, und ebenso alte, jedoch in Teilen bislang unerfüllte Forderungen neu aufgestellt, wenn auch ohne große Konsequenzen für die Debatte: So problematisiert etwa Felix Stalder die Vorstellung von *privacy* als einer Sphärentheorie, der „bubble theory“, die Relativität der individuellen „privacy notions“ oder die Tatsache, dass es auch Informationen gebe, von denen die Betroffenen gerade wollen, dass sie von den Datenverarbeiterinnen verarbeitet werden, und fordert eine Abkehr von einer solchen „ever-weakening illusion of privacy“ und das Vertreten der Forderung nach „accountability of those whose power is enhanced by the new connections.“[1624] Neu sind eigentlich nur der postmoderne Impetus und stetige Neuerfindung von Begriffen für Dinge und Konzepte, die es schon lange vorher gab.[1625]

Vor dem Hintergrund der von ihm als Fehlstelle identifizierten „entwickelte[n] Geschichte oder gar Soziologie des Datenschutzes“ versucht Martin Rost Anfang der 2000er Jahre auf der Basis der Beobachtung, dass Datenschutz „Kommunikationen, an denen Organisationen beteiligt sind,

[1619] Siehe zu dieser Selbstbeschränkung Petronio (2002, S. xv), Stanton und Stam (2003, S. 154) oder Palen und Dourish (2003, S. 129).

[1620] Das gilt selbst für Arbeiten, die sich mit dem Einfluss Altmans auf die *privacy*-Debatte beschäftigen, siehe etwa Margulis (2003).

[1621] Das hält die Vertreterinnen dieser Theorieschule jedoch nicht davon ab, aus diesen Theorien Folgerungen für die Interaktion mit Organisationen zu ziehen, siehe etwa Hartzog und Stutzman (2013, S. 405), und diese dabei zugleich wieder auszublenden, wie sich anhand der Darstellung von Tumblr zeigt.

[1622] So David Lyon im Editorial zur ersten Ausgabe der neuen Zeitschrift „Surveillance & Society“, siehe Lyon (2002, S. 1).

[1623] Marx (2001, S. 157, Fn. 1). Siehe auch Marx (2002).

[1624] Siehe Stalder (2002a, S. 122 f.).

[1625] Das zeigt sich etwa bei Haggerty und Ericson (2000, S. 606), in der sie mit Gilles Deleuze und Félix Guattari von einer „emerging »surveillant assemblage«“ sprechen und damit im Grunde ein *kontingentes System* meinen, das „operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct »data doubles« which can be scrutinized and targeted for intervention.“ Für eine ironische Kritik an solchen Ansätzen siehe Morningstar (1993).

unter Bedingungen“ stelle, die gesellschaftliche Funktion des Datenschutzes soziologisch zu theoretisieren.[1626] In einer „systemtheoretische[n] Lesart der Evolution sozialer Systeme“ – segmentär strukturierte gefolgt von stratifizierten und dann funktional differenzierten Systemen – analysiert er die „um sich greifende[] Industrialisierung der Informationsverarbeitung in Organisationen“, die „tendenziell zu einer Restratifizierung der Gesellschaft“ führe, „weil der inhärente funktionale Impuls von Organisationen, die Umwelt der Organisation, allein aus Verwaltungs- und Transferkostenersparnisgründen, der organisationsinternen Struktur entsprechend zu entwerfen, wieder gute Chancen auf Realisierung hat“, und identifiziert als Funktion des Datenschutzes, „dafür zu sorgen, dass die gesellschaftlichen Struktur- und Leistungsgewinne, die sich im Zuge der sozialen Evolution durch funktionale Differenzierung einstellen, durch zunehmende Restratifizierungszumutungen seitens der Organisationen nicht wieder verloren gehen.“ Datenschutz sei dabei sowohl „Entropiewächter“ zum Schutz vor gesellschaftlicher Entdifferenzierung wie „Modernisierungsagent, der weitere Strukturdifferenzen einzieht.“[1627] Als zentralen Mechanismus zur Sicherstellung der Aufrechterhaltung der in einer funktional differenzierten Gesellschaft „weitgehend kontingente[n] Wahl einnehmbarer Rollen“ sieht er die Verhinderung „einer Verkettung von differenzierten Kommunikationen“. Während „in der nicht-technisierten sozialen Wirklichkeit“ moderner Gesellschaften diese Nichtverkettung etwa in Form von Anonymität grundsätzlich gegeben sei,[1628] müsse sie unter den Bedingungen einer technisch vermittelten Kommunikation explizit durch Technik erzeugt werden.[1629]

2.5.5 Der Markt soll es richten

Warren und Brandeis hatten ihr *privacy*-Konzept auf der Beobachtung, dass die traditionelle eigentumsbasierte Schutzarchitektur von *privacy* mit den neuen technischen Entwicklungen an ihre Grenzen gestoßen sei, aufgebaut und daher einen persönlichkeitsrechtlichen Ansatz gewählt.[1630] Damit war die Diskussion allerdings nicht beendet. Stattdessen gab es in großen Wellen immer wieder Vorschläge, das *privacy*- oder Datenschutzproblem durch den Markt richten zu lassen, vorwiegend – jedoch nicht ausschließlich – über Eigentums- oder eigentumsähnliche Konstruktionen.[1631]

[1626] Siehe dazu und zum folgenden Rost (2002), wenn nicht anders verwiesen. Wieviele – und welche – der Arbeiten aus der Datenschutdebatte der 1970er Jahre Rost zu diesem Zeitpunkt bereits kennt, ist unklar. Zitiert wird nur das Steinmüller-Gutachten. Später wird er nicht nur eine große Zahl von Interviews mit Beteiligten aus der ersten Generation der Datenschützerinnen führen, etwa mit Podlech (Rost und Krasemann (2008)), Steinmüller (Rost und Krasemann (2009)) und Müller (Rost (2012a)), sondern gerade auch deren Arbeiten seine eigenen systemtheoretischen Analysen einordnen, siehe dazu vor allem Rost (2013b), Rost (2014a) und Rost (2014b): Die historische Datenschutzdiskussion sei fundiert, aber beschränkt, denn sie beziehe sich noch auf den Luhmann vor der „autopoietischen Wende“, so Rost in einem persönlichen Gespräch. Die englischsprachige Debatte, und dabei insbesondere die konzeptionell verwandten Arbeiten von Rule, ignoriert er bislang – aus welchen Gründen auch immer – weitgehend. Siehe auch Tække (2011) zur Verbindung zwischen Clarkes von Rule beeinflusstes Konzept der *dataveillance*, den Surveillance Studies und Luhmanns Systemtheorie in der Analyse von Organisationsmacht.

[1627] Siehe dazu auch ausführlicher Rost (2008a). Es gehe um die „Konditionierung asymmetrischer Machtbeziehungen“, Rost (2013b, S. 85).

[1628] Siehe dazu gesondert Rost (2003b) und Rost (2003a).

[1629] Siehe dazu auch umfassend Rost (2004).

[1630] Siehe Warren und Brandeis (1890).

[1631] Die erste, wenn auch kurze, Welle hat Westin (1967) losgetreten. Die zweite Welle lässt sich wohl mit Posner (1978a), Posner (1978b), Posner (1981) und Stigler (1980) verbinden. Die dritte Welle beginnt dann in den 1990er Jahren und umfasst etwa den schon betrachteten Lessig (1999). Alle diese Wellen haben auch jeweils

Die Auseinandersetzung ist besonders durch zwei Eigenschaften gekennzeichnet: erstens die geringe Lernfähigkeit aller Beteiligten, besonders, aber nicht nur der Marktlösungsverfechterinnen, die sich etwa darin zeigt, dass die immer gleichen Vorschläge für eine Lösung über den Markt[1632] auf immer gleiche Kritiken treffen, und zweitens die komplette Ignoranz gegenüber der Tatsache, dass in einer auf dem Prinzip individueller Autonomie basierenden Rechtsordnung einer bürgerlichen Gesellschaft eigentums- und persönlichkeitsrechtliche Operationalisierungsansätze notwendig strukturähnlich sein müssen.[1633]

Marktansätze treten dabei vorwiegend in zwei Formen auf – als Vorschläge für einen Markt, auf dem personenbezogene Informationen als handelbare Güter getauscht werden, und als Vorschläge für einen Markt, der PETs erzeugt und handelt oder nutzt und damit wirbt –, wobei die Grenzen zwischen beiden allerdings fließend sind. Die konkreten Vorschläge beziehen sich dabei notwendig auf konkrete, jedoch oft nicht explizierte Vorstellungen über das Schutzgut.[1634] Viele dieser Vorschläge zielen auf eine Institutionalisierung von bestimmten Intermediären – entweder in der Form von „information banks“, „information exchanges“ und „information clearinghouses“[1635] oder in der Form von Zertifizierungsagenturen und Auditoren, die dann Siegel wie TRUSTe oder EuroPriSe vergeben.[1636]

Dabei vertreten einige der Marktbefürworterinnen die Ansicht, es bedürfe eines – teilweise durchaus strengen – staatlichen Eingriffs zur Erzeugung eines Marktes, während andere auf eine (fast) reine Selbstregulierung setzen[1637] und gar fordern, dass der Staat schlicht die Ergebnisse von Aushandlungsprozessen in vermachteten Verhältnissen zugunsten der sozial Mächtigen, die

ihre Kritikerinnen produziert, siehe etwa Miller (1969, S. 1223 ff.), Seidel (1970, S. 1583), Steinmüller (1975c, S. 144), Podlech (1975b, S. 73), Steinmüller (1981, S. 166), Simitis (1998, S. 2476 f.) und Weichert (2001).

[1632] Siehe etwa Novotny und Spiekermann (2013) für einen neueren Versuch, alten Wein in neuen Schläuchen zu verkaufen. Vor allem eines hat sich im Laufe der Zeit gar nicht verändert: Immer noch lautet die zentrale Begründung, „[p]roperty rights would create stronger asset awareness in the minds of all stakeholders“, siehe S. 1642, auch wenn noch nie untersucht wurde, für welche *privacy*-Vorstellungen das gilt und für welche nicht.

[1633] Daraus erklären sich auch die Fehleinschätzungen über die Entwicklung von Rechtsregimen, siehe etwa Victor (2013). Dieser Aspekt kann hier aus Platzgründen aber nicht weiter ausgeführt werden, nur so viel: Sowohl die Privatautonomie wie das Recht auf informationelle Selbstbestimmung sind Ausprägungen des allgemeinen Autonomierechts und werden im Recht auch strukturell ähnlich operationalisiert, nämlich als Information über spätere Handlungen und auf der Basis dieser Information getroffener Willenserklärung. Angebot und Annahme im Kaufvertragsrecht entsprechen Information und Einwilligung im Datenschutzrecht (oder „notice and consent“ im *privacy law*). Gleiches gilt für das Recht auf körperliche Unversehrtheit und seine Umsetzung im Bereich der ärztlichen Heilbehandlung, aus der die spezifische Operationalisierung im *privacy*- und Datenschutzrecht übernommen wurde, siehe Pohle (2015b) und Pohle (2016b). Damit wird deutlich, dass sich jeweils ein Konzept, aber auch jeweils ein Operationalisierungsansatz, in einem relativ weiten, aber nicht notwendig im gesamten, Anwendungsbereich in eines der anderen Konzepte und dessen Operationalisierung abbilden lässt. Mehr noch als der Nachweis der grundsätzlichen Transformierbarkeit der Konzepte und Operationalisierungen muss hier eine genaue Bestimmung der Bedingungen offenbleiben, unter denen diese Transformationen konkret möglich ist.

[1634] Siehe schon die Ausführungen bei Agre (1999), aber auch Purtova (2009), die zeigt, wie sehr die Definition des Problems, das eine Propertisierung lösen soll, die Lösung produziert. Ganz deutlich wird das etwa bei Bibas (1994, S. 605), dessen vertragsrechtlich konstruierte Lösung schlicht Folge seiner A-priori-Annahme ist, dass *privacy nur* einen ökonomisch bestimmbaren Wert habe.

[1635] Siehe etwa Laudon (1996) mit seinem Vorschlag für einen „National Information Market“ mit „Local Information Banks“ und „National Information Exchanges“.

[1636] Immer, wenn diese Zertifizierungssysteme tatsächlich untersucht werden, stellt sich heraus, dass sie nicht halten, was sie versprechen, siehe etwa Clarke (2001), LaRose und Rifon (2006), van Goethem et al. (2014) und Connolly et al. (2014). Leider gibt es nicht zu allen Zertifizierungssystemen Untersuchungen – so fehlt etwa das von vielen Datenschutzaufsichtsbehörden unterstützte und aktiv beworbene „Europäische Datenschutzgütesiegel“, so Bock (2008), „European Privacy Seal“ (EuroPriSe).

[1637] Siehe etwa Etzioni (1999b, S. 160 ff.) oder Kilian (2002).

schon gesiegt haben, normiere in der Form, „dass staatliche Maßnahmen nur in Abstimmung mit den Selbstorganisationsprozessen der betroffenen Industrien und Dienstleistungsunternehmen erfolgen können.“[1638]

Am Ende sind bisher alle Markt- und Selbstregulierungsansätze wenig überraschend gescheitert, wobei es allerdings keine Einigkeit darüber gibt, was die Ursachen für dieses Scheitern sind. Alles ist schon als Begründung angeboten worden, von Staatsversagen, weil der Staat keinen oder keinen funktionsfähigen Markt kreiert habe, über Eigenschaften von Informationen als Waren bis hin zur Interessenkonstellation und den Anreizstrukturen im Bereich der organisierten Informationsverarbeitung.[1639]

2.5.6 Privacy by Design und Architekturvorschläge

Im Verlaufe der 1990er und zu Beginn der 2000er Jahre wurde eine Reihe von Arbeiten zum Prozess der Gestaltung *privacy-* und datenschutzfreundlicher Systeme vorgelegt, die durchaus eng mit der allgemeinen Debatte in der Informatik zu Vorgehensweisen und Technikgestaltungsmethoden verzahnt ist, insbesondere wenn es darum geht, aus Zielen beteiligter Akteurinnen oder Dritter technische Anforderungen abzuleiten und dabei im Laufe dieses Prozesses Abwägungen zwischen konfligierenden Zielen vorzunehmen.[1640]

Ein frühes Modell in diesem Zusammenhang ist das von Batya Friedman und Kolleginnen vorgeschlagene „Value Sensitive Design“:[1641] Danach sollen in einem iterativen Vorgehen konzeptuelle, empirische und technische Analysen zusammengebracht werden, um „values“ – die durchgängig nur „philosophisch“ begründet, nicht aber wirklichkeitswissenschaftlich substantiiert werden[1642] – in die Technikgestaltung einfließen zu lassen. Die konzeptuelle Analyse soll dabei die zu verfolgenden „values“ identizieren und miteinander abwägen, die dann durch empirische Untersuchungen – etwa zu welchen Abwägungsergebnissen Nutzerinnen und Betroffene kommen – unterstützt werden. Technische Untersuchungen sollen dann etwa aufdecken, welche „technological properties and underlying mechanisms support or hinder human values.“

Etwa zur gleichen Zeit wurden formale Beschreibungen von „Privacy Impact Assessments“ vorgelegt, deren Entwicklungsgeschichte bis in die 1970er Jahre zurückreichen soll.[1643] Sie sollen weiter reichen als reine Audits und eine echte Folgenabschätzung liefern, um nicht nur die Übereinstimmung mit oder Verletzung von Gesetzen feststellen, sondern deren Angemessenheit selbst auch hinterfragen zu können. Sie können sich dabei auf ganz unterschiedliche Konzepte von *privacy* beziehen[1644] Das Vorgehen soll systematisch und zugleich umfassend sein, den Prozess der Systemgestaltung wie das System als Produkt betrachten, die jeweils angemessene

[1638] Siehe Vesting (2003, S. 188 ff.).

[1639] Siehe – ohne Anspruch auf Vollständigkeit – Culnan (2000), Vila et al. (2003), Hoofnagle (2006), Bonneau und Preibusch (2010), Rossnagel (2010), Swire (2012) und Bock (2014).

[1640] Siehe dazu etwa Dardenne et al. (1993) und van Lamsweerde (2001).

[1641] Siehe grundlegend Friedman (1996), für ein frühes Anwendungsbeispiel siehe Friedman et al. (2000) und zur Vorgehensmethode, die nachfolgend dargestellt wird, siehe Friedman et al. (2002). Siehe auch den von Friedman herausgegebenen Sammelband „Human Values and the Design of Computer Technology“, Friedman (1997).

[1642] So betrachten die Autorinnen das „right to privacy“ schlicht als „moral value“, siehe Friedman et al. (2002, S. 2).

[1643] Siehe Stewart (1996), zur Geschichte siehe Clarke (1999), Flaherty (2000), Warren et al. (2008) und Clarke (2009).

[1644] So schon die Kritik von Clarke (1999). Siehe auch den umfassenden Sammelband Wright und De Hert (2012), indem sich die Beiträge, wenn sie überhaupt so weit gehen, auf Informationsflusskontrolle im engeren Sinne, also Geheimhaltung und Vertraulichkeit – und insoweit klassische IT-Sicherheitsziele –, sowie Zweckbindung beschränken.

Expertise einbeziehen und zugleich unabhängig sein – oder zumindest alle Interessen offenlegen – sowie direkt in den Entscheidungsprozess über die Gestaltung oder Einführung des neuen Systems eingebunden sein. Im Laufe der Zeit sind dann auch konkrete Vorgehensmodelle vorgelegt worden, etwa ein sechsschrittiges Modell von Oetzel und Spiekermann in Zusammenarbeit mit dem BSI: (1) Festlegung des Untersuchungsgegenstandes, (2) Identifikation der „privacy targets" – eine etwas willkürliche und jedenfalls juristisch nicht fundierte Auswahl aus in der EG-DSRL statuierten Anforderungen –, (3) Schutzbedarfsfeststellung für jedes „privacy target", (4) Bedrohungsanalyse für jedes „privacy target", (5) Identifikation der Mittel Minimierung, Abschwächung oder Abwehr der Bedrohungen und (6) Bewertung und Dokumenation der verbleibenden Risiken.[1645] Nicht nur wählen die Autorinnen nur eine Teilmenge der durch das Recht adressierten Anforderungen aus,[1646] sie prüfen sie auch nur einzeln und unabhängig voneinander.[1647] Wenig überraschend ist Kritik an diesen verkürzten PIAs laut geworden: „Ungeklärt ist oft die Unabhängigkeit der Autoren und die Verallgemeinerungsfähigkeit und Relevanz der Modelle, fragwürdig sind darin vor allem die Validität und Reliabilität der genutzten Kriterien, mit denen Datenschutzrisiken operationalisiert und analysiert werden", insbesondere fehle eine Analyse der „Risiken für die informationelle Selbstbestimmung durch die Machtasymmetrie zwischen Organisationen und Personen".[1648] Rost und Bock schlagen daher vor, in einem ersten Schritt explizit zu machen, welches Ziel das PIA verfolge: (1) Evaluation eines Produktes oder Verfahrens, „ohne dass im Vorhinein ein bestimmtes Set an Kriterienkatalogen und Definitionen sowie Angreifermotive festgelegt sind", (2) vollständige Compliance mit dem Datenschutzrecht und (3) mit wissenschaftlichem Anspruch, also „Risiken vollständig, sowohl empirisch verlässlich als auch mit einem hohen prognostischen und spekulativen Anteil theoretisch gestützt und methodisch zu erfassen", indem „neben den Perspektiven des Betroffenen und der Organisation(en) auch die der gesellschaftlichen Risiken" analysiert und bewertet werden.[1649]

In Anlehnung an das „Privacy Impact Assessment" wurde im Rahmen des „Privacy Incorporated Software Agent Consortium" ein „Design Embedded Privacy Risk Management" (DEPRM, manchmal auch DEPREM) entwickelt, das auch auf der Basis der EG-DSRL operiert und im wesentlichen die gleichen Rechtsprinzipien identifiziert wie Oetzel und Spiekermann, diese jedoch – jedenfalls zu Beginn des Projekts – nur in den Dimensionen *confidentiality*, *integrity*, *availability* und *controllability* analysiert.[1650] Im weiteren Projektverlauf wird die Methode erweitert: Aus den analysierten Rechtsquellen wird abgeleitet, wie sich das System zu verhalten habe, um diese

[1645] Siehe Oetzel und Spiekermann (2012).

[1646] Das ist eigentlich noch komplizierter: Das Recht ist stark prozedural geprägt und gibt demnach an vielen Stellen Anforderungen an die Entscheidung über die Gestaltung von Informationsverarbeitungs- und Entscheidungsprozessen vor, nicht jedoch zugleich alle Anforderungen an die Verarbeitung und Entscheidung; diese sind erst zu entwickeln, auch vor dem Hintergrund der in der Richtlinie niedergelegten Zielvorstellungen: „Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten" (Art. 1 Abs. 1).

[1647] Siehe zu diesem Problem Pohle (2014a, S. 52 ff.): Für komplexe Systeme gilt, dass das Ganze mehr ist als die Summe seiner Teile. Es fehlen demnach in diesem Vorgehensmodell geeignete Vorkehrungen, um Bedrohungen identifizieren zu können, die sich erst aus dem Zusammenspiel der einzelnen Teile ergeben.

[1648] Siehe Rost und Bock (2012, S. 743), wobei sie allerdings konzedieren, dass der Ansatz von Oetzel und Spiekermann zu den besseren gehöre, siehe S. 744. Auch das von David Wright und Charles Raab vorgeschlagene „Surveillance Impact Assessment" geht über eine solche beschränkte *privacy*-Sicht hinaus, siehe Wright und Raab (2012).

[1649] Siehe Rost und Bock (2012, S. 744 f.). So dann später auch Friedewald et al. (2016, S. 21 f.).

[1650] Siehe Kenny und Borking (2002), siehe zum Start des PISA-Projekts Borking (2001), bei dem es im Kern um die Entwicklung einer Middleware im PET-Sinne zum Schutz von *privacy* geht. Siehe zu den Grenzen des *privacy*-Verständnisses vom PETs 2.4.4, S. 173.

Verhaltensanforderungen dann in technische Anforderungen zu übersetzen, wobei die im Recht verwendeten Begriffe und Konzepte sowie deren Verhältnisse zueinander in formalisierter Form in Ontologien abgebildet werden sollen.[1651]

Mit einer Beschränkung auf die fünf Fair Information Practice Principles, die sie als „privacy protection goals“ übernehmen, und die sie um sieben „privacy vulnerability goals“ – später „privacy goal obstacles“ genannt – ergänzen, die Faktoren oder Handlungen bezeichnen sollen, die als „privacy invasions“ identifiziert werden,[1652] versucht eine Gruppe um Annie Antón und Julia Earp ein Framework für die Analyse von Privacy Policies vorzulegen, das sie dann erweitern, um damit *privacy*-Anforderungen in der Modellierung von Rollen und Berechtigungen im Rahmen von RBAC-Systemen (Role-Based Access Control) abbilden zu können.[1653] Eine weitere Erweiterung erfolgt dann in einem größeren Projekt durch Annie Antón und Colin Potts, indem sie nicht nur die Abbildbarkeit von Pflichten hinzunehmen, sondern auch eine Formalisierung anstreben, die es ermöglicht, mit Hilfe von Software – „Run-Time Tools“ – die Einhaltung der Policies durchzusetzen.[1654] Ein ähnliches Vorgehen, aber auf der Basis der OECD-Guidelines, wählen Eric Yu und Luiz Marcio Cysneiros, wobei sie allerdings mit ihrem Modell in der Lage sind, *privacy* und mithin die sich daraus ergebenden Anforderungen, aus der Sicht der verschiedenen beteiligten Stakeholder jeweils getrennt zu modellieren und damit auf eine A-priori-Definition verzichten zu können.[1655] Und Ann Cavoukian stützt sich auf das „Canadian Standards Association Model“, das große Überschneidungen zu den OECD-Guidelines und der EG-DSRL aufweist, und schlägt dafür dann „Privacy Design Principles“ vor.[1656] Diesen Ansatz arbeitet sie später zu ihrem erfolgreich verkauften „Privacy by Design“ aus, das auf sieben grundlegenden Prinzipien beruhe: „[1] Proactive not reactive; Preventative not remedial, [2] Privacy as the default setting, [3] Privacy embedded into design, [4] Full functionality – positive-sum, not zero-sum, [5] End-to-end security – full lifecycle protection, [6] Visibility and transparency – keep it open, [7] Respect for user privacy – keep it user-centric“.[1657] Seda Gürses, Carmela Troncoso und Claudia Diaz weisen völlig zu Recht darauf hin, dass das Konzept komplett vage ist,[1658] und das ist eigentlich noch untertrieben: Nicht nur enthält es überhaupt keine Ausführungen zum methodologischen Vorgehen, es fehlt auch schlicht an einer ordentlichen Operationalisierung von Anforderungen – es handelt sich eher um einen Mummenschanz.

Neben den Vorgehensweisen und Technikgestaltungsmethoden wurden Architekturen und Systeme diskutiert, die für eine Durchsetzung der Anforderungen in der Datenverarbeitung sorgen sollen, sowie formale Sprachen, mit denen sich die dazu erforderlichen Regeln formulieren lassen. Bei IBM entwickelte eine Gruppe um Günter Karjoth und Matthias Schunter die „IBM Enterprise Privacy Architecture“ (EPA) auf der Basis eines zentralen Berechtigungsmonitors mit dem Ziel, „to maximize the business use of personal information while respecting priva-

[1651] Siehe vor allem van Blarkom et al. (2003, S. 169 ff.). Die Ontologie, die im Rahmen des Projektes entstanden sein soll, scheint nicht öffentlich verfügbar zu sein, und die Projektwebseite `pet-pisa.nl` ist offline.

[1652] Siehe Antón und Earp (2001) und Earp et al. (2002).

[1653] Siehe He und Antón (2003).

[1654] Siehe zum Forschungsplan Antón und Potts (2003). Zu den nicht sehr nachhaltigen Ergebnisse, die auch noch sehr oberflächlich bleiben und auf sehr mechanistischen Vorstellungen von Recht basieren, jedenfalls aber keine „Run-Time Tools“ hervorgebracht zu haben scheinen, siehe Breaux und Antón (2005), Jensen et al. (2005), Breaux et al. (2006), Breaux und Antón (2007) und Otto und Antón (2007).

[1655] Siehe Yu und Cysneiros (2002), Yu und Cysneiros (2003) sowie Liu et al. (2003), auch ohne weitere Folgen.

[1656] Siehe Cavoukian (2000).

[1657] Siehe Cavoukian (2010) und Cavoukian et al. (2010).

[1658] Siehe Gürses et al. (2011, S. 3).

cy concerns and regulations.“[1659] Für die Formulierung der Regeln, nach denen der Berechtigungsmonitor die Datenverarbeitung steuern sollte, wurde anschließend die „Enterprise Privacy Authorization Language“ spezifiziert,[1660] allerdings scheint es keine Systeme zu geben, die diese Sprache unterstützen. Ein Team bei Hewlett-Packard entwickelte ein ähnliches System, das sie um „sticky policies“ erweiterten, die HP dann patentierte, und sogar in Produkte von HP implementierte.[1661] Und Larry Korba und Steve Kenny untersuchen, ob und inwieweit sich Digital-Rights-Management-Systeme (DRM) als „Privacy Rights Management for individuals“ (PRM) auf der Basis der EG-DSRL einsetzen lassen,[1662] aber auch dieser Ansatz scheint keine praktischen Auswirkungen gehabt zu haben, genauso wenig wie das ISTPA Privacy Framework oder Carnival.[1663]

2.5.7 Nutzerkontrollierbare Systeme

Die in den 1990ern an Fahrt gewinnende Debatte zur Gestaltung von *privacy*-freundlichen Systemen, die nicht auf Rechnern von Datenverarbeiterinnen, sondern auf Rechnern von Betroffenen laufen, bettet sich einerseits in ein viel breiteres Interessenfeld im Bereich des „Computer Supported Cooperative Work“ ein, andererseits gibt es aber auch sehr viele Überschneidungen mit der Debatte um PETs, insbesondere dort, wo die PETs auf nutzerkontrollierbare und nutzerkontrollierte Systeme setzen.[1664] Im Vergleich zu der vorher weit verbreiteten Selbstbeschränkung der Gestaltungsdiskussion auf Systeme, die unter der Kontrolle von Datenverarbeiterinnen laufen, verschieben sich dann auch die Anforderungen an die technischen Systeme, wenn Betroffene sind jetzt nicht mehr nur *usees*, sondern gerade auch *user* sind. Insbesondere wird *privacy* damit auch zu einem Problem des UI-Designs. Victoria Bellotti und Abigail Sellen stellen vor diesem Hintergrund „feedback“ und „control“ als Designprinzipien auf.[1665] Dabei definieren sie „feedback“ als Prinzip des Informierens der Nutzerinnen darüber, wann und welche Informationen jeweils erhoben und wem sie übermittelt werden, während „control“ die Eigenschaft von Systemen bezeichnet, Nutzerinnen sinnvolle Steuerungsmöglichkeiten darüber an die Hand zu geben, welche Informationen sie jeweils preisgeben und an wen, und mappen die beiden Prinzipien dann auf die vier von ihnen als relevant identifizierten Aspekte der Informationsverarbeitung: „capture“, „construction“, „accessibility“ und „purpose“. Andrew Clement baut darauf auf und verweist auf die in der CSCW-Debatte bislang ignorierten Fair Information Practice Principles, hält für den wichtigsten Punkt allerdings die Einbindung der Betroffenen in den Entwicklungsprozess, in

[1659] Siehe Karjoth et al. (2002).

[1660] Siehe Ashley et al. (2003).

[1661] Siehe dazu Mont et al. (2003b), Mont et al. (2003a) und Mont et al. (2005). Die Idee der „sticky policies“ stammt von Miller (1971, S. 144) und hätte daher eigentlich gar nicht patentierbar sein dürfen. Inzwischen werden sie, wie Hansen (2014b, S. 79, Rn. 28) berichtet, zwar in vielen Forschungsprojekten eingesetzt, so etwa im Projekt „PRIME – Privacy and Identity Management for Europe“, siehe Casassa Mont (2006a) und Casassa Mont (2006b), finden dann aber – wegen der Patentierung – ihren Weg nicht in die Praxis. Und nach einer Produktsuche auf HPs Webseite nach zu urteilen, wurden alle Produkte, in die diese Ideen implementiert wurden, im Laufe der Zeit abgekündigt.

[1662] Siehe Korba und Kenny (2002).

[1663] Siehe zum Privacy Framework der „International Security, Trust and Privacy Alliance“ ISTPA (2002) und ISTPA (2007) sowie zu Carnival Arnesen und Danielsson (2003) und Arnesen et al. (2004).

[1664] Siehe etwa Schmidt und Bannon (1992), die *privacy* unter dem Label „opaqueness“ diskutieren (S. 35). Diese Zuschreibung wird später von Paul de Hert und Serge Gutwirth wieder aufgenommen, die der konzeptionellen Gleichsetzung „privacy = opacity of the individual“ die Gleichsetzung „data protection = transparency of power“ gegenüberstellen, siehe De Hert und Gutwirth (2006).

[1665] Siehe Bellotti und Sellen (1993).

dem die Eigenschaften der zu entwickelnden Systeme tatsächlich verhandelbar sein müssen.[1666] Einen Schritt weiter geht Dag Wiese Schartum und fordert die Entwicklung von nutzerkontrollierten Werkzeugen, die mindestens sechs Bereiche abdecken sollen: (1) die Opt-In-/Opt-Out-Verwaltung für das Abgeben und Zurückziehen von Einwilligungen, (2) die Durchsetzung der Informationsfreiheit im Sinne der Rezipientinnenfreiheit, (3) den Zugriff auf die über sich selbst gespeicherten personenbezogenen Informationen, (4) den Zugriff auf Informationen über das interne Verhalten von Systemen und Verfahren, (5) das Verhindern, zum Objekt automatisierter Einzelfallentscheidungen zu werden, und (6) die Information, wenn personenbezogene Informationen bei Dritten erhoben werden.[1667] Ein Versuch, einen Teil dieser Anforderungen umzusetzen, unternehmen David Nguyen und Elizabeth Mynatt mit ihrem Vorschlag für einen „Privacy Mirror“, der Nutzerinnen in die Lage versetzen soll, das soziotechnische System, mit dem sie interagieren und das Informationen über sie sammelt, verarbeitet und nutzt, zu verstehen und zu beeinflussen. Dazu soll das System die Informationsflüsse sichtbar machen, die sonst vor der Nutzerin versteckt ablaufen.[1668] Im Rahmen der Entwicklung einer Methode zur „Privacy Interface Analysis“ versuchen auch Andrew Patrick and Steve Kenny, für das PISA-Projekt passende User Interfaces zu entwickeln, um Nutzerinnen verständlich zu informieren, auf das sie angemessen reagieren können[1669]

2.5.8 Das Privacy Paradox

Fast nirgends sonst lässt sich so gut beobachten, wie fragwürdig die Wissenschaftlichkeit der ganzen *privacy*-, *surveillance*- und Datenschutzdebatte war und ist, wie in der Causa „Privacy Paradox“.

Die Frage, wer den Begriff des Privacy Paradox zuerst nutzte und zur Beschreibung welchen Sachverhalts, wird sich wohl nicht mehr klären lassen, jedenfalls aber wurde der Begriff in sehr viel mehr Kontexten gebraucht, als sein heutiges Verständnis – zur Bezeichnung der Diskrepanz zwischen den von Individuen geäußerten *privacy*-Bedenken und ihrem tatsächlichen Verhalten – nahelegt.

Anfang 1998 nutzte das „Reporters Committee for Freedom of the Press“ den Begriff, um damit die Beschränkung der Pressefreiheit zugunsten eines verstärkten *privacy*-Schutzes zu problematisieren[1670] – mit teils absurden Beispielen wie „wiretapping and eavesdropping are illegal in most states even if done for the purpose of gathering news“, indem sie fordern, dass Journalistinnen unbedingt auf Gesundheitsdaten aller Patientinnen zugreifen müssten, denn „[i]dentification of individuals strengthens the impact and credibility of newsworthy articles“, indem sie beklagen, dass Vergewaltigungsopfer in Strafverfahren inzwischen ein Recht auf Anonymität hätten, oder indem sie behaupten, der Erste Zusatzartikel zur US-Verfassung verbiete jede staatliche Regulierung jedes „exchange of truthful information in the first place.“[1671] Im gleichen Jahr behauptet Joseph Kizza, das Privacy Paradox bestehe darin, dass „too much individual privacy

[1666] Siehe Clement (1994).

[1667] Siehe Schartum (2001, S. 162) mit der Begründung, das europäische Datenschutzrecht basiere auf „awareness and active data subjects who are capable of exercising their legal rights in an information society where the traffic of personal data knows no European borders.“ Die Verantwortung für die Entwicklung der Werkzeuge sieht er dabei in erster Linie bei den Datenschutzaufsichtsbehörden, siehe S. 167.

[1668] Siehe Nguyen und Mynatt (2002).

[1669] Siehe Patrick und Kenny (2003). Den Bildern in dem Artikel nach zu urteilen, war die Entwicklung allerdings nicht von Erfolg gekrönt.

[1670] Siehe Kirtley (1998).

[1671] Siehe Kirtley (1998, S. 4, 9, 11 und 15).

is very dangerous“, denn „if each individual has total privacy, then society as a whole has zero security.“[1672] Und im Jahre 2001 behauptet Fred Cate, das Privacy Paradox bestehe in der Nichtnutzung der von Verbänden und Lobbyorganisationen angebotenen „»opt-out« programs“ durch Betroffene bei gleichzeitiger Angabe, dass sie „worried about their privacy“ seien,[1673] während Eric Jorstad mit dem Privacy Paradox die „ambivalence“ bezeichnen will, die darin liege, dass „we“, also „americans“, gleichzeitig an einen abgeschlossenen „private space“ und „a free market and free speech regime“ ohne „out-moded barriers“, wo „no question, no comment, no product, is out of bounds“, glauben.[1674] Diese Gebrauche des Privacy Paradox sollen hier, obwohl sie es durchaus auch verdient hätten, nicht adressiert werden.

In der Literatur zum Privacy Paradox wird häufig eine Untersuchung von Lorrie Faith Cranor, Joseph Reagle und Mark Ackerman als erste Arbeit zum Privacy Paradox genannt,[1675] obwohl der Begriff dort gar nicht auftaucht. In einer webgestützten Umfrage fragten die Autorinnen die Einstellungen der Befragten zur *privacy* auf der Basis von Szenarien ab und kommen unter anderem zum Ergebnis, dass Nutzerinnen mehr Informationen über sich preisgeben, wenn diese anonym erhoben werden, und dass ganz grundlegend sehr viele Faktoren die Preisgabewahrscheinlichkeit beeinflussen, darunter ob die Informationen an Dritte weitergegeben werden, welche Informationen überhaupt erhoben werden und für welche Zwecke das geschieht – überhaupt wird sehr konkret auf die Zweckbezogenheit und Zweckgebundenheit der Preisgabeentscheidung verwiesen. Wenn diese Studie hingegen zitiert wird, dann nicht mit einem dieser differenzierten Ergebnisse, sondern immer mit einer sehr pauschalen Aussage aus dem Einleitungsabsatz zur Darstellung der Ergebnisse – „General Attitudes about Online Privacy“:

> „Overall, our respondents registered a high level of concern about privacy in general and on the Internet. Only 13% of respondents reported they were »not very« or »not at all« concerned. Nonetheless, while the vast majority of our respondents were concerned about privacy, their reactions to scenarios involving online data collection were extremely varied. Some reported that they would rarely be willing to provide personal data online, others showed some willingness to provide data depending on the situation, and others were quite willing to provide data – regardless of whether or not they reported a high level of concern about privacy. Thus it seems unlikely that a one-size-fits all approach to online privacy is likely to succeed.“[1676]

Barry Brown hingegen bezeichnet etwas später die Gleichzeitigkeit von Beschwerden von Betroffenen über die Gefährdung ihrer *privacy* und ihrer Nutzung von Supermarkt-Kundinnenkarten, die die Aussage von Cranor, Reagle und Ackerman zu stützen scheint, explizit als Privacy Paradox,[1677] während Tara Radin – natürlich in einer ethischen Betrachtung – behauptet, dass „[p]rivacy, at least in part, encompasses the goal of being left *alone*. The simple act of engaging

[1672] Siehe Kizza (1998, S. 154 f.).

[1673] Siehe Cate (2001, S. 3). Hier handelt es sich um ein ganz anderes Problem, nämlich das der Nichtänderung von Voreinstellungen in der Praxis, siehe dazu Johnson et al. (2002) und Willis (2014) das inzwischen zur weitverbreiteten Forderung nach „Privacy by Default“ geführt hat, die etwa in der neuen EU-DSGVO in Art. 25 Abs. 2 auch umgesetzt wurde.

[1674] Siehe Jorstad (2001, S. 1503 f.).

[1675] Die Arbeit wurde zweimal veröffentlicht, einmal als technischer Report der AT&T Labs, siehe Cranor et al. (1999), und einmal als Beitrag zur 1st ACM Conference on Electronic Commerce, siehe Ackerman et al. (1999). Unglücklicherweise sind der Fragebogen und die Frequenz der Antworten, die im Report verlinkt sind, nicht mehr online.

[1676] Cranor et al. (1999) und Ackerman et al. (1999, S. 2).

[1677] Siehe Brown (2001).

in e-commerce, though, indicates that people actually want to interact with others“, und gerade das sei das Privacy Paradox, denn „[a] person truly concerned with *privacy* is not surfing the net or engaging in e-commerce.“[1678] Und auch Sarah Spiekermann, Jens Grossklags und Bettina Berendt sowie Alessandro Acquisti und Grossklags stellen in ihren Untersuchungen eine solche Diskrepanz fest, ohne sie jedoch explizit als paradox zu bezeichnen.[1679]

Popularisiert wurde der Begriff Privacy Paradox jedoch erst durch einen Artikel von Susan Barnes, in dem sie das Verhalten von – vor allem jugendlichen – Nutzerinnen auf Social-Media-Plattformen reflektiert und eine „paradoxical world of privacy“ beschreibt: „On one hand, teenagers reveal their intimate thoughts and behaviors online and, on the other hand, government agencies and marketers are collecting personal data about us.“ Das Problem sei, so Barnes, dass „[s]tudents may think that their Facebook or MySpace journal entries are private but they are actually public diaries.“[1680] Und Patricia Norberg, Daniel Horne und David Horne, die im Gegensatz zu Barnes tatsächlich (zwei) Studien durchführten, führen das Privacy Paradox darauf zurück, dass die Verhaltensabsicht und das tatsächliche Verhalten betreffend die Preisgabe von personenbezogenen Informationen nicht von den gleichen Faktoren beeinflusst würden, sondern die Absicht vorwiegend Produkt der individuellen Risikowahrnehmung sei, während die tatsächliche Preisgabe in erster Linie von einer Vertrauensheuristik gesteuert werde.[1681]

Begriff, Inhalt und Begründung des Privacy Paradoxes sind jedoch in den letzten Jahren durchaus verstärkt in die Kritik geraten, vor allem als zu wenig differenzierend. Alyson Leigh Young und Anabel Quan-Haase zeigen mit einer Differenzierung nach *social privacy* – in Interaktionssystemen – und *institutional privacy* – zwischen Individuen und Organisationen –, dass das Verständnis der Betroffenen stark zugunsten der *social privacy* verzerrt ist, während die Betroffenen nur wenig Problembewusstsein in Bezug auf die *institutional privacy* hätten, zugleich aber im Bereich der zwischenmenschlichen Beziehungen eine relative Konsistenz zwischen den Intentionen und den tatsächlichen Handlungen bestehe.[1682] Zu einem ähnlichen Ergebnis kommen auch Christoph Lutz und Pepe Strathoff, die unter Verweis auf Tönnies *social privacy* mit Gemeinschaft und *institutional privacy* mit Gesellschaft verbinden,[1683] um dann sogar einen Schritt weiter zu gehen: Das Privacy Paradox erscheine gar nicht mehr paradox, weil die „emotional geprägte Suche nach Gemeinschaft“, die sich in der Preisgabe von personenbezogenen Informationen etwa auf Facebook verwirkliche, stärker sei „als die Abgrenzung in der Gesellschaft im Sinne der Privatsphäre und die damit verbundenen Befürchtungen um Privacy-Gefahren.“[1684] Andererseits zeigt Young Min Baek in einer Serie von Experimenten, in denen den Probandinnen zwischen je zwei Befragungen Gegenargumente vorgelegt wurden, dass die meisten Menschen gar keine gefestigte Meinung zu *privacy* und den damit zusammenhängenden

[1678] Siehe Radin (2001, S. 160 f.).
[1679] Siehe Spiekermann et al. (2001) und Acquisti und Grossklags (2003).
[1680] Barnes (2006).
[1681] Siehe Norberg et al. (2007).
[1682] Siehe Young und Quan-Haase (2013). Die Unterscheidung zwischen „social“ und „institutional privacy“ wird von Raynes-Goldie (2010) übernommen. Tatsächlich ist sie aber viel älter: Es ist die Unterscheidung zwischen den informationellen Aspekten des allgemeinen Persönlichkeitsrechts, die im Datenschutzrecht geregelt sind, und denen, die es nicht sind. Nicht im Datenschutzrecht geregelt sind nämlich alle Informationsverarbeitungen durch Personen und Gruppen zu persönlichen und familiären Zwecken oder für persönliche und familiäre Tätigkeiten und somit ein Großteil dessen, was von Raynes-Goldie unter „social privacy“ verstanden wird. Hier zeigt sich wieder beispielhaft, dass sowohl die einzelnen Disziplinen wie die einzelnen nationalen Wissenschaftsdiskurse hochgradig ignorant sind gegenüber Erkenntnissen und Entwicklungen in anderen Disziplinen und Diskursen.
[1683] Siehe Lutz und Strathoff (2013).
[1684] Siehe Strathoff und Lutz (2015, S. 210 f.).

Gefährdungen haben, vor allem nicht diejenigen mit geringeren Kenntnissen, und dass in diesem Zusammenhang gar kein Privacy Paradox auftrete.[1685] Und zuletzt erklären Tobias Dienlin und Sabine Trepte das Privacy Paradox sogar für gelöst, indem sie einerseits zwischen „informational", „social" und „psychological privacy" trennen, andererseits zwischen „privacy attitudes" und „privacy concerns", und dann feststellen, dass das Privacy Paradox „disappears".[1686]

In allen Fällen wird – manchmal sehr offen und manchmal nur implizit – *privacy* als *Zustand* betrachtet, in dem sich die Betroffenen nicht mehr befinden, wenn sie Informationen über sich preisgegeben haben. In diesem Sinne geht also *privacy* durch die Preisgabe personenbezogener Informationen verloren. Dies geschieht selbst dann, wenn entweder die zugrunde gelegte *privacy*-Theorie, die Antworten der Befragten oder beides auf ein anderes als ein zustandsorientiertes *privacy*-Konzept verweisen oder hinweisen. So legt etwa Alan Westin *privacy*-Konzept mit *privacy* als dem „claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"[1687] und das diesem Konzept entsprechende – unterkomplexe – Verständnis von informationeller Selbstbestimmung als „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"[1688] nahe, dass die Preisgabe der Informationen kein *privacy*-Verlust, sondern gerade eine Ausübung der *privacy* ist. Gleiches gilt für die auf Irwin Altman aufbauenden Konzeptionen von *privacy*, nach denen *privacy* gerade die reale Praxis des „boundary management" als einem dialektischen Prozess sei,[1689] ebenso wie für eine als Selbstdarstellung verstandene *privacy*.[1690] Und auch die *privacy*-Konzeptionen, die sich auf die Frage der Fairness in der organisationsinternen Abbildung der Person, der Fairness im Umgang mit personenbezogenen Informationen oder der Fairness in Entscheidungen über Menschen durch Organisationen beziehen,[1691] sprechen gerade gegen einen Verlust der *privacy* allein durch die Preisgabe von personenbezogenen Informationen. Vor allem aber ignoriert die Forschung zum

[1685] Siehe Baek (2014).

[1686] Siehe Dienlin und Trepte (2015). Die Unterscheidung zwischen „informational", „social" und „psychological privacy" ist mehr als arg konstruiert und findet keine Entsprechung in der sonstigen *privacy*-Debatte. Und dafür gibt es einen guten Grund: Die Autorinnen fragen unter dem Label „informational privacy" zur Preisgabe von „identifying information", unter dem Label „social privacy" zur Sichtbarkeit des Profils und unter dem Label „psychological privacy" zur Preisgabe von „personal information" (S. 289) – alle drei Aspekte werden in der allgemeinen *privacy*-Debatte unter „informational privacy" behandelt. Weder die Dreiteilung noch die Grenzziehung zwischen werden ordentlich begründet (S. 286) mit dem Ergebnis, dass die unter „informational privacy" gefasste Frage „How precisely do you want to be identifiable for strangers on FB?" (S. 289) eigentlich eher unter „social privacy" gehören müsste, denn diese „captures the dialectic process of regulating proximity and distance toward others" (S. 286).

[1687] Westin (1967, S. 7).

[1688] BVerfG (1983, S. 43). Dieses Verständnis ist nicht *per se* unterkomplex, sondern nur unterkomplex im Vergleich zu Steinmüllers Regelkreismodell für die Beeinflussung von Freiheitsräumen, siehe Steinmüller et al. (1971, S. 87).

[1689] Siehe Altman (1975) und Petronio (2002).

[1690] Siehe etwa Britz (2007). Dieser Topos der Selbstdarstellung ist bereits extrem früh in der *privacy*- und Datenschutzdebatte angelegt, nämlich schon in den zugrunde gelegten soziologischen Theorien, siehe Goffman (1956) – im Englischen als „The Presentation of Self in Everyday Life" erschienen, im Deutschen als „Wir alle spielen Theater. Die Selbstdarstellung im Alltag" – und Luhmann (1986) – bei dem Würde zugleich „Grundbedingung[] des Gelingens der Selbstdarstellung" (S. 61) und Ergebnis „gelungene[r] Selbstdarstellung" (S. 68) ist – , wird aber auch schon seit den 1970ern breit diskutiert, siehe etwa Schmidt (1974), Podlech (1975b) – und die anderen Beiträge Podlechs – sowie Meister (1983).

[1691] Siehe etwa U.S. Department of Health, Education, and Welfare (1973), Laudon (1986a), Lyon (1994) und Nissenbaum (2004) für Arbeiten, die vor oder während der Privacy-Paradox-Diskussion erschienen, sowie Citron (2008), Ochs und Löw (2012), Capurro et al. (2013) und Dwork und Mulligan (2013) für spätere Arbeiten.

Privacy Paradox, dass die jeweiligen Preisgaben von Informationen grundsätzlich nicht bedingungslos erfolgen, sondern – jedenfalls wenn es sich um eine gemäß den meisten *privacy*- und Datenschutzgesetzen legale Datenverarbeitung handelt – beschränkt sind auf konkrete Kontexte und Zwecke, in die vor oder mit der Preisgabe explizit oder implizit eingewilligt wurde.

Das Privacy Paradox, so wie es in allen diesen Arbeiten beschrieben wurde und wird, kann deshalb konzeptionell nur dann vorliegen, wenn *privacy* ein Zustand ist, der durch die Preisgabe personenbezogener Informationen zwingend verlassen wird, wenn – wie in James Rules Konzept von *privacy* – die Verarbeitung personenbezogener Informationen durch Organisationen *per definitionem* als Verletzung der *privacy* der Betroffenen betrachtet wird oder wenn *privacy* nichts anderes als Geheimhaltung bedeutet.

Vor diesem Hintergrund stellt sich natürlich die aus Platzgründen leider hier nicht diskutiert werden könnende Frage, warum dann auch so viele Vertreterinnen von *privacy*-, *surveillance*- und Datenschutztheorien an die Existenz dieses Privacy Paradoxes glauben. Eine mögliche Erklärung könnte sein, dass es sich bei allen diesen Theorien um „Schaufenster-Theorien" handelt, die nur vorgeschoben sind, weil sie vermeintlich wissenschaftlicher wirken, ihre Vertreterinnen jedoch – im Grunde ihres Herzens – von einer zustandsorientierten Theorie ausgehen, einem von der Welt und der Gesellschaft abgeschlossenen Rückzugs-„Raum" des Individuums.[1692]

2.6 Noch mehr alter Wein in neuen Schläuchen und aufkommende Kritik

Im Anschluss an die Anschläge vom 11. September 2001 in New York – und dann jeweils in gesteigerter Form nach den Anschlägen vom 11. März 2004 in Madrid und vom 7. Juli 2005 in London – kam eine inzwischen sehr alte Diskussion zu neuen Weihen, die durch die Gegenüberstellung von Sicherheit und Freiheit geprägt ist und wenig überraschend mit einem Sieg der Sicherheit über die Freiheit endet.[1693] In der Folge wurde eine Vielzahl neuer Überwachungsgesetze und -instrumente eingeführt. In der Bundesrepublik zählten und zählen dazu etwa die Vorratsdatenspeicherung, die Online-Durchsuchung oder der Bundestrojaner, die dann jeweils Gegenstand umfassender politischer und wissenschaftlicher – und teilweise vor dem Bundesverfassungsgericht und anderen Höchstgerichten ausgetragener – Auseinandersetzungen waren und sind.[1694]

Ein wesentlicher Teil der Debatte im neuen Jahrtausend fokussierte auf alten und neuen Techniken moderner Informationsverarbeitung: den „Resten" des Ubiquitous Computing, bevor es als Thema vom Internet of Things abgelöst wurde, Personalisierung und Tracking, immer noch und doch wieder neu entdeckt auch Profilbildung und Scoring, dazu dann Big Data und das alte und zugleich neu entdeckte Problem der Algorithmisierung. Parallel fand eine nicht enden wollende Diskussion um eine Reform des Datenschutzrechts statt, wobei die Reförmchen, die es stattdessen gab, nur Flickwerk bleiben,[1695] bis im Januar 2012 die EU-Kommission einen Entwurf für eine Datenschutzgrundverordnung vorstellt.[1696] Die nationalen Reformdiskussionen kommen

[1692] Und in den empirischen Untersuchungen taucht es dann eben auf, weil dementsprechend die „falschen" Fragen gestellt werden – eine Tatsache, die schon Paul Müller kritisiert hat, siehe Müller (1975a, S. 129). Auch spätere Kritik in dieser Richtung, siehe etwa Bull (2004, S. 85 ff.), bleibt ungehört.

[1693] Siehe dazu und zum folgenden Hetzer (2006) und vor allem Singelnstein und Stolle (2012).

[1694] Siehe beispielhaft etwa Kahler (2008), Petri (2008), Hensel (2009), Schmale und Tinnefeld (2012), Rehak (2014), Moser-Knierim (2014).

[1695] Siehe etwa Tauss et al. (2004) und Fox (2009).

[1696] Europäische Kommission (2012), siehe auch den Überblick bei Hornung (2012).

damit fast schlagartig zum Erliegen, und alles dreht sich um die Europäische Datenschutzreform, die im April 2016 beschlossen wurde.[1697]

Dann gab Edward Snowden einen weiteren kleinen Einblick in die Praxis westlicher Massenüberwachung,[1698] und (fast) alle waren überrascht – oder gaben sich zumindest den Anschein, überrascht zu sein. Massive Änderungen wurden gefordert,[1699] aber am Ende passierte, was in der Vergangenheit – vielleicht mit Ausnahme des Church Committees und seiner Folgen[1700] – immer passierte: Die illegalen Machenschaften der Dienste wurden ein klein wenig zurückgestutzt, im wesentlichen aber einfach legalisiert.[1701] Das wird nicht nur am Fall „Schrems“ deutlich: Max Schrems gewann vor dem EuGH, der mit seinem Urteil „Safe Harbor“ den Todesstoß versetzte, das daraufhin durch ein ebenso löchriges „Privacy Shield“ ersetzt wurde.[1702]

2.6.1 Von 9/11 über Big Data bis Edward Snowden

Obwohl die konkrete Entwicklung im Bereich des Datenschutzes sowohl vor wie nach dem 11. September deutlich in Richtung seiner faktischen Abschaffung zeigt, vor allem im Bereich der Sicherheitsbehörden und der Geheimdienste,[1703] aber auch im Bereich der Wirtschaft,[1704] zeigen sich gerade die Datenschützerinnen fast schon übertrieben optimistisch.[1705] Vielleicht sind es jedoch gerade die „Rückzugsgefechte“ selbst, die eine Reaktion hervorrufen, die je nach Kontext weniger als Optimismus, sondern eher als „Pfeifen im Walde“ und teilweise als Trotz bezeichnet werden müssen.[1706] Letzteres gilt etwa für Simitis, der es für absurd hält, dass die Datenschutzgesetze „weder die Zunahme der Verarbeitung noch die schier unaufhaltsame Proliferation der Daten verhindert, sondern nachhaltig gefördert“ hätten.[1707] Dieser Kritik liegt eine

[1697] Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). ABl. L 119 vom 4. Mai 2016.

[1698] Siehe statt vieler Beckedahl und Meister (2013).

[1699] Siehe etwa Hansen (2014a).

[1700] Siehe Murphy (2014).

[1701] Siehe schon Steinmüller (1979a) für den Geheimdienstbereich sowie Denninger (1985, S. 215 f.) und Denninger (1987, S. 127 ff.) zu den „Folgen“ des Volkszählungsurteils. Siehe auch zur Aufdeckung von Echelon vor allem Campbell (2000).

[1702] Siehe zum Überblick Kuner (2016).

[1703] Siehe zu diesem die Datenschutzdebatte seit Anbeginn prägenden Grundkonflikt Garstka (2004, S. 5 ff.). Und selbst die wenigen verbleibenden Schutzmechanismen funktionieren nicht, wie Rachor (2004) für den Richtervorbehalt zeigt.

[1704] So Petri (2004), der nicht zu erklären vermag, warum die Regelungen, die für ihn „in der Theorie gut sind, in der Praxis indes keinen effektiven“ Grundrechtsschutz erzeugen (S. 233). So ist etwa die von ihm, vor allem aber von Büllesbach (2004) als Mechanismus bejubelte Selbstregulierung eine konzeptionelle Totgeburt, wie Hoofnagle (2006) oder Swire (2012) zeigen.

[1705] Siehe etwa Weichert (2004), der fordert, dass Datenschutz Spaß machen solle, obwohl er zugleich konzedieren muss, dass Datenschutz mit seinem „dienende[n] Charakter“ (S. 143) nur Bedingung der Möglichkeit, also „Voraussetzung für Spaß“, aber nicht Spaß selbst ist. Am extremsten wird dieser – naive – Optimismus bei Roßnagel (2004) deutlich, der 2004 glaubt, dass bis 2015 „wichtige Herausforderungen [...] bewältigt“ sein würden (S. 335). Roßnagels Vorhersage ist ebenso wie Bulls Einschätzung, es sei äußerst unwahrscheinlich, „dass Unternehmen individuelle Persönlichkeitsprofile zur massenhaft gezielt-individuellen Nutzung herstellen [würden]; der Aufwand wäre viel zu groß“, Bull (2004, S. 90), ein gutes Beispiel dafür, dass die dystopischen Vorhersagen der Datenschützerinnen weit realistischer sind als die utopischen.

[1706] Siehe Mertens (2006) für eine Begründung auf der Basis einer Trennung in „Datenschutz im Großen“ und „Datenschutz im Kleinen“, wonach das Zurückdrängen des Datenschutzes in gesellschaftlich zentralen Bereichen durch „Parkinsonsche Effekte“ „in weniger wichtigen Sektoren“ (S. 416) kompensiert würde.

[1707] Simitis (2005, S. 519). Zu einem ähnlichen Ergebnis für das Datenschutzrecht insgesamt, also länderübergreifend, kommt Koops (2014).

Gleichsetzung des Ziels des Datenschutzes – Beschränkung von Informationsmacht über Menschen – mit dem Mittel, dessen sich das Recht zu seiner Erreichung bedient – Kontrolle über die Informationen, die diese Menschen abbilden oder abbilden sollen –, zugrunde. Anstatt jedoch an dieser Stelle anzusetzen und diese Gleichsetzung zu kritisieren, werden ihr einfach andere Gleichsetzungen entgegengesetzt – oder sogar die gleiche, etwa bei der Frage nach Profilbildung, die nur dann für relevant erachtet wird, wenn das Profil korrekt ist.[1708]

Die Folgen einer solchen Gleichsetzung zeigen sich dann etwa im Umgang mit Datenschutzaudits, aber auch in vergleichbarer Form in Bezug auf Privacy Policies. Unter solchen Bedingungen degenerieren Datenschutzaudits dann nicht selten zu reinen Daten*sicherheits*audits – und die Beteiligten sind auch noch stolz darauf.[1709] Ähnliches gilt für ein Datenschutzmanagement, bei dem Datenschutz nur durch die Brille der IT-Sicherheit und ihrer Konzepte betrachtet wird:[1710] erstens schon nur als Substitut zweiter Ordnung (Datenschutz → Datenschutzrecht → Datenschutzrecht nach IT-Grundschutz), zweitens aber auch in Bezug auf die Rangordnung zwischen Sicherheit und Datenschutz.[1711] Und im Umgang mit Privacy Policies produziert diese Gleichsetzung dann sowohl auf Seiten der solche Policies untersuchenden Wissenschaftlerinnen wie auch auf Seiten der Betroffenen Fehlverständnisse und falsche Erwartungen.[1712]

Die innerdeutsche Diskussion um die Reform des Datenschutzrechts hat – ausgelöst durch einige Datenschutzskandale – im Jahr 2009 zu drei sehr kleinen Novellierungen geführt, die dann wieder breit juristisch diskutiert wurden.[1713] Dabei stehen sich unterschiedliche Forderungen nach einer grundsätzlichen Neukonzeption des Datenschutzrechts ebenso gegenüber wie in verschiedene Richtungen drängende Detailänderungen. Simitis fordert etwa, alle allgemeinen Regelungen im BDSG zu treffen und die bereichsspezifischen „durchweg darauf abgestimmt und bezogen“ zu gestalten.[1714] Darüber hinaus fordert er eine quasi binäre Regulierung: Zwecke und Verarbeitungsbedingungen seien gesetzlich verbindlich und abschließend zu regeln, Ausnahmen wie zweckfremde Verarbeitung dürften nicht zulässig sein.[1715] In einer Stellungnahme des Ber-

[1708] So etwa Bull (2006, S. 1622), dessen Beispiele für „harmlose“ – siehe dazu auch den dritten Fall bei Hoofnagle (2007) – Informationsverarbeitungen schon damals von der Praxis widerlegt waren, vor allem weil er bei seiner „Analyse“ immer nur bei den unselbständigen Zwischenprodukten von Entscheidungen stehen bleibt – geostatistische Marktforschungsergebnisse werden nämlich nicht, wie Bull unterstellt (S. 1620), nur zum Versand von Werbung verwendet, sondern auch zur Preisgestaltung oder sogar zur Einstellung des Angebots in den „aussortierten“ Gebieten, siehe dazu etwa Grötker (2006, S. 56 f.). Es geht gerade nicht nur darum, wie Bull suggeriert (S. 1618) und damit eigenen früheren Äußerungen – Bull (1984, S. 85) – widerspricht, bestimmte „Anwendungen von Technik“ zu problematisieren, sondern die sich daraus ergebenden Machtverhältnisse und -verschiebungen zwischen sozialen Akteurinnen, siehe Buchner (2006, S. 28 ff., 51 ff.).

[1709] Siehe Behrendt (2006).

[1710] Siehe Meints (2006) und Simon (2007).

[1711] Siehe zu letzterem Rost (2013a), der daher das Datenschutzmanagementsystem ausgehend vom Datenschutz – und nicht von der IT-Sicherheit – konzeptionalisiert.

[1712] Siehe zum ersten LaRose und Rifon (2006) sowie zum zweiten Turow et al. (2006) und Custers et al. (2013), die daraus jeweils Regulierungsbedarf ableiten.

[1713] Siehe zur Übersicht über die Änderungen Eckhardt (2009) und zum Ausblick auf die – aus damaliger Sicht – noch kommenden Novellierungen Fox (2009).

[1714] Siehe dazu und zum folgenden Simitis (2007, S. 151 ff.). Ein solches Vorgehen, das im übrigen in der Softwareentwicklung Usus ist – alles Wiederkehrende wird ein Mal festgelegt (normiert oder programmiert) und dann aufgerufen und dabei nur dort mit Differenzregelungen versehen, wo dies notwendig ist –, würde zugleich dem Anspruch an eine Kodifikation genügt werden. Siehe zu diesen Ansprüchen und dem Scheitern des bestehenden Datenschutzrechts an diesen Ansprüchen von Lewinski (2011).

[1715] Das Verbot mit Erlaubnisvorbehalt, das Simitis hier noch verschärfen will, wird immer wieder kritisiert, siehe etwa die auf Bulls technisch uninformierten und rechtlich unreflektierten Angriff auf das Datenschutzrecht, Bull (2013), in dem Bull zugleich nachweist, dass er seit Bull (2009) nichts gelernt hat, folgende Auseinandersetzung (Weichert (2013), Kramer (2013), aber auch Karg (2013), Giesen (2013), und Brink (2014)). Ebenso umstritten

liner Datenschutzbeauftragten vor dem Bundestags-Innenausschuss schlägt Alexander Dix nach der „Gefahrenträchtigkeit“ von Informationsverarbeitungsvorgängen, etwa nach der „Nähe der Daten zum Persönlichkeitskern von Betroffenen“, abgestufte Regelungen vor, ohne dabei allerdings diesen „Persönlichkeitskern“ bestimmen zu können – und das angesprochene Beispiel des Auskunfteiwesens bietet das gerade nicht.[1716] Und für das ULD statuiert Johann Bizer zwar, dass „[d]as derzeitige Schutzkonzept wird den Herausforderungen nicht im erforderlichen Umfang gerecht“, verweist dann aber nicht auf konzeptuelle Probleme, sondern nur auf die Unübersichtlichkeit des Rechts, einzelne Schutzlücken und das Problem des Vollzugsdefizits, um dann einen „Datenschutz durch Technik“, Audit- und Zertifizierungsverfahren sowie ein „Prozessmanagement“ zu fordern.[1717]

Die Rufe nach einer Überarbeitung des Datenschutzrechts werden nach den Novellierungen 2009 nicht leiser: Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt Simitis' Forderung nach einem BDSG als „Allgemeinem Teil“ des Datenschutzrechts auf der Basis von „Schutzzielen“ und „Grundsatznormen“, „die für alle Formen der Datenverarbeitung gleichermaßen gelten“ sollen wie der Grundsatz der Zweckbindung oder ein neu einzuführendes „grundsätzliches Verbot der Profilbildung“.[1718] Dieses Verbot der Profilbildung ist dabei nicht der einzige Vorschlag, der in der Diskussion neu aufgewärmt wird. Gleiches gilt etwa für das Vergessen, seine rechtliche Normierung und seine Umsetzung in Technik,[1719] dessen „Erfindung“ in der neueren Debatte zum „right to be forgotten“ vor allem Viktor Mayer-Schönberger zugeschrieben wird.[1720] Seitdem feiert es jedenfalls in der Debatte fröhlich Urständ – mit teils sehr extremen Beiträgen von allen Seiten[1721] – und hat es am Ende sogar in die EU-Datenschutzgrundverordnung geschafft, wenn auch nur in einer Überschrift, denn die Norm selbst statuiert nicht mehr als ein Recht auf Löschung, wie es seit den 1970er Jahren im deutschen und später auch im europäischen Datenschutzrecht umgesetzt wurde.[1722]

---

ist und bleibt die Zweckbindung, siehe etwa Eifert (2007) und von Grafenstein (2015), die aber nur die Konsequenzen für die Datenverarbeiterinnen ausleuchten, nicht jedoch die Folgen für den Zweck, dem das Prinzip der Zweckbindung dienen soll, sowie Pohle (2015b). Nach dem BKAG-Urteil des BVerfG vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, ist die „hypothetische Datenneuerhebung“ die verfassungsrechtlich gebotene Operationalisierung des Zweckbindungsgrundsatzes (Rn. 287). Die Frage, ob sich diese Operationalisierung auch auf Private anwenden lässt, kann hier nicht diskutiert werden.

[1716] Siehe Dix (2007).

[1717] Siehe Bizer (2007c) sowie etwas ausführlicher Bizer (2007a). Dieser hier Prozessmanagement genannte Ansatz, siehe auch Bizer (2006a), Bizer (2007b) und Meints (2007), ist keineswegs neu, sondern liegt dem Datenschutzrecht schon seit Anbeginn zugrunde – es ist nichts anderes als die Umsetzung der Phasenorientierung des Datenschutzrechts in der Organisation, um die Gesetzesbefolgung zu ermöglichen. Siehe ausführlich Steinmüller (1993, S. 225 ff.).

[1718] Siehe Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2010). Es ist allerdings unklar, was hier – vor allem in Abgrenzung zu Grundsatznormen – mit Schutzzielen adressiert werden soll. Die Formulierung zur Technikneutralität der rechtlichen Regelungen – „technikneutrale Vorgaben [...], die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen werden“ – spricht eher für das aus der IT-Sicherheit bekannte Konzept von Schutzzielen, wie es von Rost und Pfitzmann (2009) auf den Datenschutz übertragen und entsprechend angepasst wurde.

[1719] Siehe schon Stone und Warner (1969, S. 260), Podlech (1973a, S. 59 ff.), Schlink (1973, S. 165 ff.) und Chaum (1985c, S. 1042) für Auseinandersetzungen zu diesem Problem.

[1720] Siehe Mayer-Schönberger (2009), entwickelt wohl schon 2007, siehe Mayer-Schönberger (2007), und unter anderem vorgetragen auf einem Symposium mit dem Titel „Glücklich ist, wer vergisst[...]“ in Mainz, siehe Wagner (2008).

[1721] Siehe beispielhaft Shoor (2014), Kulk und Borgesius (2014), Korenhof et al. (2015) und Rustad und Kulevska (2015).

[1722] Siehe Zanfir (2015).

Weil einerseits die Datenschutzdebatte schon immer von der Auseinandersetzung mit den Sicherheitsbehörden und Nachrichtendiensten geprägt war[1723] und andererseits die Aufdeckung und öffentliche Diskussion von Echelon sowie die oben schon angerissenen Auseinandersetzungen um die nach dem 11. September 2001 eingeführten oder ausgeweiteten Überwachungsgesetze und -instrumente noch hätten frisch in Erinnerung sein müssen,[1724] überrascht der relativ große Aufruhr, den Edward Snowden mit seinen Enthüllungen verursacht hat, sehr. Die Debatte ist von einer relativen Dreiteilung gekennzeichnet, die sich zwar nicht in drei streng getrennten Phasen, jedoch in drei zeitlichen Schwerpunkten beobachten lässt: Zu Beginn gab es einen Schwerpunkt auf der Beschreibung und Analyse der von Snowden und anderen enthüllten massiven Überwachung des weltweiten Kommunikationsverkehrs durch US-amerikanische – und wie dann aufgedeckt wurde, auch andere vor allem westliche – Geheimdienste, während gleichzeitig die politische Diskussion – oder besser: die Simulation einer politischen Diskussion – zwischen einer breiten Verurteilung dieser Maßnahmen vor allem von Oppositionsseite und einer weitgehenden Abwiegelung durch die verantwortlichen Regierungen oszillierte.[1725] Der zweite Schwerpunkt wurde durch die Versuche gekennzeichnet, auf verschiedenen Ebenen dieses Problem der Massenüberwachung technisch, politisch und/oder rechtlich zu lösen, und war geprägt von einem durchaus weitverbreiteten Optimismus hinsichtlich einer grundsätzlichen Lösbarkeit.[1726] Und die tatsächlich vorgenommenen Änderungen in den Gesetzen, aber auch in den Überwachungsorganisationen, stellen dann den dritten Schwerpunkt dar, wobei im Ergebnis in den meisten Fällen die vormals illegalen oder jedenfalls in einer rechtlichen Grauzone vollzogenen Überwachungsmaßnahmen legalisiert wurden oder sich gerade im Prozess der Legalisierung befinden.[1727] So gesetzliche Beschränkungen eingeführt wurden, bezogen sie sich fast ausschließlich auf die jeweils eigenen Bürgerinnen.[1728] Die Nähe von Erfolg und Misserfolg beim Versuch, geheimdienstliche Massenüberwachung rechtsstaatlich unter Kontrolle zu bringen, zeigt der breit diskutierte Fall „Schrems“: Obwohl nicht nur in der wissenschaftlichen Debatte schon lange die Einschätzung vorherrschte, dass „Safe Harbor“ ein Papiertiger sei, der den europäischen Betroffenen keinen Grundrechtsschutz bieten könnte, bedurfte es erst des EuGH, um aus der Nacktheit des Kaisers Konsequenzen zu ziehen. Während auf der einen Seite das Urteil als großer Erfolg gefeiert wurde, beschleunigte die andere Seite die nach den Snowden-Enthüllungen begonnenen Verhandlungen über Regelungen zu staatlichen Zugriffen auf von privaten Anbieterinnen gehaltenen Daten im transatlantischen Datenaustausch, die Anfang 2016 in einem als „Privacy Shield“ bezeichneten Ersatz des „Safe Harbor“-Abkommens mündeten, der die zentralen Probleme gar nicht angeht

[1723] Siehe etwa Garstka (2004), Hirsch (2008) und Hirsch (2011).

[1724] Siehe etwa GegenStandpunkt (2006).

[1725] Das ist zugleich der Schwerpunkt der publizistischen und wissenschaftlichen Auseinandersetzung, siehe beispielhaft Beckedahl und Meister (2013), Reidenberg (2013), Newell (2014) und Cohen (2014).

[1726] Siehe etwa die Lösungsvorschläge bei Bigo et al. (2013, S. 32 ff.), Hansen (2014a), Froomkin (2015) und Zalnieriute (2015). Im technischen Bereich hat etwa die IETF damit begonnen, existierende RFCs vor dem Hintergrund der nach den Snowden-Enthüllungen vorgenommenen Anpassungen der Angreifermodelle neu zu evaluieren, siehe dazu und zu den bereits überprüften RFCs die „perpass“-Mailingliste für die IETF-Diskussionen zu „pervasive monitoring“, https://www.ietf.org/mailman/listinfo/perpass. Siehe auch zur Analyse der einander gegenüberstehenden Positionen Robinson (2014).

[1727] Siehe dazu nur den von Netzpolitik.org am 6. Juni 2016 veröffentlichten „Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes“, https://netzpolitik.org/2016/wir-veroeffentlichen-den-gesetzentwurf-zur-bnd-reform-grosse-koalition-will-geheimdienst-ueberwachung-legalisieren/#Gesetzentwurf, abgerufen am: 6. Juni 2016.

[1728] Siehe die Darstellung bei Swire (2015).

und diese Tatsache etwa durch die Einführung einer zahnlosen, weil unter anderem auf der Basis einer einseitigen Entscheidung der US-Regierung umgehbaren, Ombudsperson nur vernebelt.[1729]

Eine andere Entwicklung, die mittelfristig größere Auswirkungen auf die tatsächlichen Möglichkeiten staatlicher Stellen zu Massenüberwachung und dem massenweisen Zugriff auf bei privaten Dritten gespeicherte personenbezogene Informationen haben könnte, stellt die EU-Datenschutzreform dar, die zugleich spätestens mit der Vorstellung eines Vorschlags für eine Datenschutzgrundverordnung (DSGVO) durch die EU-Kommission im Januar 2012[1730] die fast ausschließlich auf die Bundesrepublik fixierte Reformdiskussion der Vorjahre zum Erliegen brachte.[1731] Die verschiedenen Entwürfe und Zwischenstände sind ebenso oft hoch gelobt wie tief verdammt worden und waren gleichzeitig Gegenstand heftiger Versuche von Lobbygruppen verschiedener Art, Einfluss auf die Inhalte und Formulierungen zu nehmen.[1732] Im April 2016 wurde die DSGVO dann verabschiedet.[1733] Die zentrale Änderung gegenüber der EG-Datenschutzrichtlinie von 1995 ist, dass die Grundverordnung direkt gilt und nicht erst in nationales Recht umgesetzt werden muss.[1734] Die Grundverordnung enthält sehr viele neue Einzelregelungen,[1735] aber – vor allem auch im Vergleich zum geltenden deutschen Datenschutzrecht – wenig substanziell Neues, das in den Gegenstandsbreich dieser Arbeit fällt, vielleicht abgesehen vom Recht auf Datenübertragbarkeit (Art. 20) und der Datenschutz-Folgenabschätzung (Art. 35), wobei allerdings noch

[1729] Siehe etwa Boehm (2016). Für Nichtjuristinnen zum besseren Verständnis ein Vergleich: Ein gerichtliches Verfahren, das einfach unterbrochen werden kann, wobei dann alle in den Keller gehen, um die Beschuldigte bis zum Geständnis zu foltern, um dann mit dem Geständnis das Verfahren fortzuführen, ist nicht *ein bisschen weniger* rechtsstaatlich, sondern *das Gegenteil von einem rechtstaatlichen Verfahren.* Ebenso wäre eine wissenschaftliche Beweisführung, in der ein Beweisschritt enthalten ist mit „Das hat mir mein Gott heute Nacht im Schlaf verkündet!“ nicht einfach *ein bisschen weniger* wissenschaftlich. . .

[1730] Siehe Europäische Kommission (2012). Siehe zur Übersicht über den Vorschlag Hornung (2012) und Schild und Tinnefeld (2012).

[1731] Diese durchaus optimistisch – vielleicht auch zu optimistisch – klingende Vorhersage speist sich weniger aus konkreten einzelnen Regelungen als vielmehr aus einer Gesamtschau der Veränderungen der Anreize für Datenverarbeiterinnen. Zusammen mit einer etwas stärkeren öffentlichen Debatte und relativ vielen Entwicklungen im Bereich der Entwicklung konkreter Systeme, die staatliche Überwachungsmaßnahmen erschweren, drängt die DSGVO die Datenverarbeiterinnen in Richtung einer zunehmenden technischen wie organisatorischen Abschottung gegen staatliche Zugriffe und zugleich einer Beschränkung der Folgen, wenn doch Zugriffe stattfinden, insoweit als tendenziell weniger oder zumindest für Sicherheitsbehörden weniger relevante Informationen zur Verfügung stehen könnten.

[1732] Nicht nur würde es den Rahmen der Arbeit sprengen, diese Diskussion umfassend darzustellen, das meiste davon ist auch informatisch schlicht nicht relevant – oder sollte wegen mangelnder Qualität dem Vergessen anheim gegeben werden wie die Äußerung eines Bundesverfassungsrichters, der die Informationsfreiheit für ein Bürgerinnenrecht hält, siehe Masing (2012, S. 2307). Das ist in zweierlei Hinsicht absurd: Erstens würde daraus mit an Sicherheit grenzender Wahrscheinlichkeit folgen, dass Organisationen ebenso wenig Grundrechtsträgerinnen dieses Grundrechts sein können wie des Wahlrechts oder des Demonstrationsrechts. Zweitens sind die Bürgerinnen selbst weder die vom Datenschutz problematisierten Verarbeiterinnen, noch im Allgemeinen Normadressatinnen des Datenschutzrechts.

[1733] Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union, L 119/1.

[1734] Aus juristischer Sicht fehlt in diesem Satz ein „grundsätzlich“, aber die rechtwissenschaftliche Diskussion zum verbleibenden oder nicht verbleibenden Umsetzungsspielraum, siehe etwa von Lewinski (2012), liegt außerhalb des Rahmens dieser Arbeit.

[1735] Die daraus folgende Komplexität des Rechts wird daher auch gesehen, siehe etwa Koops (2014, S. 254 f.). Aus der Vollharmonisierungstendenz innerhalb des europäischen Mehrebenensystems, die aus dem Übergang zur Verordnung folgt, und der Vollharmonisierungstendenz hinsichtlich des Gegenstandsbereichs könnte gefolgert werden, dass es sich bei der Grundverordnung um den Versuch einer Kodifikation handelt – mit den möglichen Folgen für die „Restlaufzeit“, siehe von Lewinski (2011, S. 115).

unklar ist, ob es sich bei letzterem praktisch auch um mehr handelt als die jetzt schon geregelte Vorabkontrolle (§ 4d Abs. 5 BDSG). Trotz der „neuen“ – oder jedenfalls groß klingenden – Begriffe „Datenschutz durch Technikgestaltung“ und „Datenschutz durch datenschutzfreundliche Voreinstellungen“ (Art. 25) handelt es sich dabei um zwei grundsätzlich bereits existierende Regelungen.[1736] Auch die Zertifizierung (Art. 42) ist im BDSG grundsätzlich bereits geregelt (§ 9a), allerdings hat es der Gesetzgeber seit Jahren versäumt, ein Datenschutzauditgesetz zu verabschieden.[1737] Darüber hinaus gibt es gegenüber dem geltenden Recht auch konzeptionelle Rückschritte.[1738] Mit der auf europäischer Ebene fortgeschriebenen Nichtdifferenzierung nach Phasen der Datenverarbeitung vergibt die DSGVO nicht nur die Möglichkeit differenzierter Regelungen, wie es sie im deutschen Recht derzeit noch gibt, sondern auch einen sinnvollen Anknüpfungspunkt für Analysen komplexer Informationsverarbeitungen, etwa im Rahmen von Datenschutz-Folgenabschätzungen.[1739] Strukturell das gleiche gilt für den Wegfall sowohl des Erforderlichkeitsprinzips wie der strikten Zweckbindung und deren Folgen für die Erzeugung von Vorhersehbarkeit und Kontrollierbarkeit.[1740] Und nicht zuletzt zeigt sich in der DSGVO sehr deutlich, wie schwierig es ist, all die Gefahren für Grundrechte und -freiheiten von Menschen sauber und verständlich zu adressieren, die durch moderne Informationsverarbeitung erzeugt oder verstärkt werden, wenn diese Gefahren sowohl konzeptionell wie auch im Versuch ihrer rechtlichen Lösung immer nur vermittelt über das Konzept der personenbezogenen Daten adressiert werden können, ganz zu schweigen von den immer noch enthaltenen „sensitiven“ Daten.[1741]

2.6.2 Geschichtsschreibung – Geschichts*neu*schreibung – Geschichts*um*schreibung

Historisch konstruierte Konzepte nehmen nicht nur direkt Einfluss darauf, wie sie in Theorie und Praxis eingesetzt und in Technik und Verfahren umgesetzt werden, sie werden auch immer wieder neu durch die Brille einer Geschichtsschreibung interpretiert – und dabei leider allzuoft auch bis zur Unkenntlichkeit verzerrt oder gar in ihr Gegenteil verkehrt. Vor diesem Hintergrund überrascht es nicht, dass die in den letzten zehn bis fünfzehn Jahren erschienenen Arbeiten, die sich wahlweise mit einzelnen Aspekten oder den großen Entwicklungslinien der *privacy*- und Datenschutz(rechts)geschichte beschäftigen, in Teilen die Geschichte schlicht neu- oder umgeschrieben haben und mit einer daraus folgenden falschen Rezeption der historischen Auseinandersetzungen, Problemdefinitionen und -lösungen die aktuellen Debatten in die Verwirrung getrieben haben. Auf der anderen Seite ist leider vielen Arbeiten, die solche Fehlvorstellungen aufdecken, ein größerer Einfluss auf die Debatte versagt geblieben.

Während etwa Marit Hansen die Geschichte der Versuche, Datenschutz durch Technik „umzusetzen oder zumindest [seine] Realisierung zu unterstützen“, tatsächlich bis in die Anfänge in

[1736] Für die erste ist das klar, siehe dazu Pohle (2015a). Letzeres geht zwar etwas über den Wortlaut – und deutlich über die herrschende Auslegung – von § 3a BDSG zur „Auswahl und Gestaltung von Datenverarbeitungssystemen“ hinaus, allerdings ließen sich „Voreinstellungen“ natürlich auch unter „Gestaltung“ subsumieren, wenn das politisch gewollt wäre – und von den Juristinnen verstanden würde.

[1737] Siehe zum Diskussionsstand Hornung und Hartl (2014).

[1738] Materielle Fragen sollen hier nicht Gegenstand der Betrachtung sein. Nicht nur wären sie in erster Linie politisch zu diskutieren, es wird wohl auch noch etwas Zeit brauchen, bis die ersten tiefgehenden Analysen vorgelegt werden, siehe aber für den Anfang De Hert und Papakonstantinou (2016). Hier geht es nur um Konzept- und Strukturaspekte und deren Bewertung aus informatischer Sicht.

[1739] Siehe zu ersterem kritisch Eckhardt und Kramer (2013), zu letzterem Pohle (2014a, S. 52 ff.).

[1740] Siehe De Hert und Papakonstantinou (2016, S. 185 f.) und Pohle (2015b).

[1741] Siehe Pohle (2016b) sowie, wenn auch mit anderer Schlussfolgerung, Koops (2014, S. 256 ff.). Siehe zur Kritik an der Konstruktion solcher Sensitivitätskategorien Simitis (1990).

den 1970er Jahren zurückzuverfolgen in der Lage ist – und leider dennoch nicht den fundamentalen Unterschied zwischen diesen Versuchen und den viel späteren PETs problematisiert – und Sandra Braman die in der heutigen Debatte extrem weit verbreitete Behauptung widerlegen kann, in den ersten Jahrzehnten der Entwicklung des Internets sei das *privacy*-Problem vor allem von den Ingenieurinnen schlicht ignoriert worden,[1742] und leider beide Arbeiten weitgehend ignoriert werden, wird James Whitmans ziemlich unsägliche Arbeit „The Two Western Cultures of Privacy: Dignity versus Liberty“[1743] überraschend breit und unkritisch rezipiert, obwohl sie inhaltlich zur *information privacy*- und Datenschutzdebatte fast gar nichts beizutragen vermag, weil sie sich im Kern mit *privacy* in einem breiten Verständnis und mit dem allgemeinen Persönlichkeitsrecht – auch in seiner ganzen epischen Breite – als dessen kontinentaleuropäischem Äquivalent beschäftigt und alle Beteiligten die jeweiligen Unterschiede zwischen *privacy* in einem weiten Verständnis und *information privacy* sowie dem allgemeinen Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung fleißig ignorieren.[1744] Damit er in seinem „Vergleich“ zu dem von ihm offensichtlich gewünschten Ergebnis kommen kann, muss er an einigen sehr deutlich sichtbaren Stellen die Geschichte umschreiben oder einfach ausblenden – oder er hat schlicht keine Ahnung, wovon er schreibt: So haben Warren und Brandeis ihr *privacy*-Konzept von Kohler übernommen, ohne es auszuweisen.[1745] Whitman scheint das nicht zu wissen und Kohlers Arbeit auch nicht zu kennen, daher schließt er aus Warren und Brandeis' Übernahme des Persönlichkeitsbegriffs, dass dieser auf einem Ehrenschutzansatz basieren würde,[1746] obwohl Kohler gerade diesen Ansatz ablehnt – und gerade deswegen auch nicht einer der Väter, sondern allenfalls einer der Onkel des allgemeinen Persönlichkeitsrechts in Deutschland geworden ist.[1747] Hingegen ist ihm die Übernahme der *privacy*-Konzeption Alan Westins durch die deutsche – und in der Folge auch durch die europäische – Debatte und deren Übersetzung in das Recht auf informationelle Selbstbestimmung kein Wort wert. Stattdessen übersetzt er den historischen deutschen Disziplinbezeichner „Nationalökonomie“ in „»national« economics“ und macht daraus „a school critical of free trade and in many ways of the free market more broadly“.[1748]

Solche Fehldarstellungen der Geschichte sind aber keineswegs nur in Ausflüssen von Nichtbeteiligten zu finden, sondern werden oft genug auch von Zeitzeuginnen vorgelegt, die es eigentlich besser wissen müssten. So behaupten etwa Büllesbach und Garstka, dass die Phasenorientierung des deutschen Datenschutzrechts eine Fortentwicklung der aus den USA vorgegebenen Grundlagen sei und zugleich das damalige Bedrohungsmodell auf Systeme fokussierte, „die kaum einen

[1742] Siehe Hansen (2004, S. 290 ff.) und Braman (2011).
[1743] Siehe Whitman (2004).
[1744] Mit einer vergleichbaren Beschränkung – und damit ebenso ungeeignet für eine Auseinandersetzung mit *information privacy* und Datenschutz – Richards und Solove (2010) und Schwartz und Peifer (2010), die sich jeweils mit Prosser (1960) und dessen Folgen beschäftigen, sowie Bloch-Wehba (2014).
[1745] Siehe schon Maass (1970, S. 15).
[1746] Siehe zur Auseinandersetzung Whitmans mit der Arbeit von Warren und Brandeis Whitman (2004, S. 1202 ff.).
[1747] Auch Simitis scheint das nicht wahrzunehmen, wenn er Warren und Brandeis ebenso wie Whitman in eine Reihe mit Gareis und von Gierke stellt, siehe Simitis (2010, S. 1990). Siehe auch Frohman (2012), der argumentiert, dass es mit dem Volkszählungsurteil zu einem „breakthrough into German constitutional thought of something very much akin to what Whitman sees as a distinctly American view of privacy designed to limit the intrusion of the state into the individual private sphere“ (S. 341) kam, der allerdings in Arbeiten von Steinmüller, C. Mallmann und Podlech schon vollzogen und im Datenschutzrecht auch schon umgesetzt gewesen sei (S. 361 ff.).
[1748] Whitman (2004, S. 1181). Das kann nur glauben, wer auch glaubt, dass „Volkswirtschaftslehre“ faschistisch sei – wegen „Volksgemeinschaft“!

Datenaustausch untereinander vornahmen“,[1749] obwohl nicht nur beides historisch falsch ist, sondern Garstka in die damaligen Debatten auch tief involviert war. Steinmüllers durchaus auch als Replik darauf zu verstehende Darstellung,[1750] an der selbst auch einiges zu kritisieren ist,[1751] räumt jedenfalls mit einigen der Fehldarstellungen auf – und produziert gleichzeitig ein ganz paar neue. Von den amerikanischen Vorarbeiten ist, wie schon gezeigt, nur die äußere Schale des informationellen Selbstbestimmungsrechts übernommen worden – im Sinne des Rechts, über die Preisgabe und Verwendung personenbezogener Informationen entscheiden zu können – sowie die diesbezügliche Phraseologie, jedoch unter gleichzeitigem Austausch der theoretischen Fundierung – von Goffmans individualistischer zu Parsons und Luhmanns strukturalistischer Rollentheorie. Und gerade in technischer Hinsicht sind eben nicht die Eigenschaften der damals eingesetzten, sondern die der für die Zukunft geplanten und von den Herstellern versprochenen Systeme zugrunde gelegt worden und das vor dem Hintergrund der schon seit den 1930ern laufenden Planungen der Staatsbürokratie für ein umfassendes Bevölkerungsinformationssystem, wie auch Steinmüller rekapituliert. Ob die recht weitgehenden Übereinstimmungen zwischen den Fair Information Practices (FIP) und dem deutschen Regelungsansatz – und dann eben auch den daraus entwickelten rechtlichen Regelwerken – nun aber daraus folgen, dass führende Personen hinter beiden Konzeptionalisierungen – unter anderem Steinmüller und Ware, aber auch Weizenbaum – ihren Hintergrund in oder ihr Interesse an Kybernetik zielführend einsetzten, es einfach dem damaligen regulierungstheoretischen Ansatz entsprach oder die Konzeption in „Records, Computers, and the Rights of Citizens“ von der in „Grundfragen des Datenschutzes“ abgeschrieben wurde,[1752] ist wohl auch deshalb nicht untersucht worden,[1753] weil selbst in den besseren Arbeiten zur Geschichte die FIP zur Grundlage aller gesetzlichen Regelungen erklärt werden.[1754] Auch Lutterbecks Auseinandersetzung mit der eigenen wissenschaftlichen Vergangenheit bleibt ambivalent: Einerseits gehört er zu den wenigen, die nicht vergessen haben, warum sich die „Privatsphäre“ nicht als Anknüpfungspunkt für eine rechtliche Regelung eignet, andererseits hält er sie trotz aller Auseinandersetzungen in den 70ern, an denen er auch beteiligt war, immer noch für das Schutzgut – natürlich ohne dafür eine Definition oder gar eine Begründung mitzuliefern.[1755] Sehr ehrlich ist jedenfalls Michael Kirby, zwischen 1978 und 1980 Vorsitzender einer Expertinnengruppe der OECD zur Ausarbeitung der „OECD Guidelines on Privacy“, und erklärt:

[1749] Siehe Büllesbach und Garstka (2005, S. 721 f.). Ebenso absurd sind die Ausführungen zum Kernbereich privater Lebensgestaltung (S. 722), der schlicht eine konzeptionelle Wiederkehr der Sphärentheorie ist, sowie zum Systemdatenschutz (S. 724), der schlicht zu technisch-organisatorischen Schutzmaßnahmen verkürzt wird.

[1750] Siehe Steinmüller (2007).

[1751] Siehe Pohle (2014a, S. 46 f.).

[1752] Siehe U.S. Department of Health, Education, and Welfare (1973) und Steinmüller et al. (1971).

[1753] Vor kurzem hat Chris Hoofnagle die Transkripte von sechs der Treffen des Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS), das den HEW-Report ausgearbeitet hat, veröffentlicht, siehe Hoofnagle (2014). Neue Erkentnisse sind daher in näherer Zukunft durchaus zu erwarten.

[1754] Siehe etwa Bonner und Chiasson (2005), die davon abgesehen jedoch eine sehr gute Darstellung vorgelegt haben – im Gegensatz etwa zu Rule (2008), Holvast (2009) oder Birnhack (2013) –, vor allem auch dazu, dass die Diskussion über die Mittel – die FIP – die Diskussion über den Zweck – das Schutzgut – weitgehend in den Hintergrund gedrängt hat. Siehe auch Gellman (2014), der zumindest feststellt, dass „[e]ven laws that predated FIPs – including the 1970 Hesse (Germany) law and even the 1970 American Fair Credit Reporting Act – reflect the main elements of FIPs“ (S. 5), auch wenn er diese Tatsache nicht analysiert. Siehe zur Entstehung der Rechtsinformatik und ihrer Einflüsse auch auf die *privacy*- und Datenschutzdebatte Bing (2007) sowie Ishii et al. (2008, S. 5–14).

[1755] Siehe Lutterbeck (2010).

> „Put bluntly, the OECD concern was that the response of European nations (and European regional institutions) to the challenges of TBDF [transborder data flows] for privacy might potentially erect legal and economic barriers against which it was essential to provide effective exceptions.“[1756]

Ganz anders agiert Simitis, der wie immer die Arbeiten anderer ausblendet und nur seine eigenen Verdienste hervorhebt, wenn er das BDSG quasi direkt aus dem HDSG, an dessen Entstehung er selbst beteiligt war, abgeleitet sieht.[1757] Im Ergebnis ist er – nicht nur wegen seiner Bekanntheit, sondern auch weil er er im Gegensatz zu anderen Datenschützerinnen der ersten Generation relativ viele Arbeiten auf Englisch publiziert hat – damit ziemlich erfolgreich in der Beeinflussung der Debatte über die Geschichte des Datenschutzes und des Datenschutzrechts, wie unter anderem die sehr umfassende Arbeit von Gloria González Fuster zeigt, die nicht nur eine direkte Verbindungslinie zwischen dem HDSG und dem BDSG 1977 zieht, sondern es auch dabei belässt und die konzeptionellen Unterschiede oder der Diskussionen, die dazu in der Bundesrepublik geführt worden sind, einfach unter den Tisch fallen lässt.[1758] Hinzu tritt, dass Fuster sich bei der Darstellung der Analysen des *privacy*- und Datenschutzproblems allein auf US-amerikanische Arbeiten aus den 1960er und von Anfang der 1970er Jahre stützt, während sie die Entwicklungen in den anderen Ländern dann nur noch durch die Brille ihrer jeweiligen Übernahmen dieser Vorarbeiten und deren Umsetzungen in nationalem Recht betrachtet.[1759]

Und während es zur Vorgeschichte von *privacy*, Privatsphäre oder Geheimsphäre und deren Schutz durch das Recht durchaus einige umfassendere Arbeiten gibt,[1760] ist die Vorgeschichte des Datenschutzes und des Datenschutzrechts als Schutz vor Datenmacht, strukturell asymmetrischen Informationsverhältnissen, vor allem im Sinne einer strukturellen Beschränkung der Datenmacht staatlicher und privater Organisationen, bisher nur von Kai von Lewinski umfassender analysiert worden.[1761]

2.6.3 Noch mehr „neue“ Gefahren

Im Rahmen der Diskussion über die Gefahren, die es jeweils abzuwehren gelte, hat die Debatte in den vergangenen zehn bis fünfzehn Jahren so gut wie alle informatischen, verarbeitungspraktischen und Geschäftsmodellentwicklungen, die in der Praxis beobachtet oder für die Zukunft vorhergesagt wurden, aufgegriffen und problematisiert – von übermäßig detailfixiert bis zu alle Details zugunsten der „großen Entwicklungslinien“ ignorierend. Wenig überraschend folgt die Debatte dabei – wenn auch durchaus mit ein wenig Verzögerung – den Hypes und ihren Begriffen. Nur selten werden dabei allerdings die jeweiligen Vorgeschichten und die historischen Vorläufer der Techniken betrachtet,[1762] die jeweils als „neu“ markiert werden, bei denen jedoch bei genauerem Hinsehen nur der Begriff jeweils neu ist – wenn überhaupt. Nicht nur ist dieses

[1756] Kirby (2011, S. 8).
[1757] Siehe Simitis (2010, S. 1995 ff.).
[1758] Siehe Fuster (2014, S. 56 ff., 59 ff.).
[1759] Siehe Fuster (2014, S. 28 ff.).
[1760] Siehe etwa Maass (1970), Flaherty (1972), Austermühle (2002) oder Petersen (2005).
[1761] Siehe von Lewinski (2009).
[1762] Siehe für eine der wenigen Ausnahmen Ambrose (2014). Dass es auch schon viel früher Ansätze einer solchen historisch-kritischen Rekonstruktion gab – oder hätte geben können, denn sie sind nie konsequent weiterverfolgt worden –, zeigt Podlechs Betrachtung des das Datenschutzproblem erzeugenden Informationsgebarens moderner Organisationen vor der Folie der „neuzeitlichen Wissenschaftskonzeption von Descartes und Hobbes“, siehe Podlech (1976a, S. 23 f.).

Verhalten wissenschaftlich mehr als fragwürdig, dabei wird auch die Chance vergeben, vergangene Lösungsvorschläge und -umsetzungen kritisch überprüfen und daraus – ob positiv oder negativ – lernen zu können.

Andererseits werden natürlich auch Diskussionen, die mit bestimmten Begriffen, Konzepten und Entwicklungen verbunden sind, weitergeführt, wobei sich dann durchaus die Schwerpunkte ändern können. Eine dieser Diskussionen beschäftigt sich mit dem Ubiquitous Computing und bleibt dabei gerade dem Anfang der 1990er Jahre eingeführten Begriff verhaftet.[1763] Gleichzeitig bekommt dieses Konzept – begriffliche eher als inhaltliche – Konkurrenz: Ambient Intelligence.[1764] Wie schon bei Ubiquitous Computing handelt es sich bei Ambient Intelligence um einen Oberbegriff, unter dem einen breites Spektrum an technischen wie soziotechnischen Systemen diskutiert werden – von RFIDs, *smart objects*[1765] bis zum Internet of Things und derem jeweiligen Einsatz in der Praxis –, deren Auswirkungen auf *privacy* und Datenschutz problematisiert wird.[1766] Daneben werden die Ubiquitous Computing und Ambient Intelligence konstituierenden Elemente auch einzeln betrachtet.[1767]

Einen Schwerpunkt in der Debatte nehmen die personenbezogenen Verarbeitungsverfahren ein, die im Rahmen von Ubiquitous Computing, Ambient Intelligence und dem Internet of Things zum Einsatz kommen. Während Rost schon recht früh dafür wirbt, die seinerzeit in der technischen Datenschutzdiskussion schon eingeführten Begriffe „Verkettung“ und „Verkettbarkeit“ – *„linkage“* und *„linkability“* – als Operationalisierung von „Beziehung“, „Herstellen einer Beziehung“, „In-Beziehung-gesetzt-Haben“ und „Beziehbarkeit“ zu verwenden,[1768] kann sich damit allerdings nicht durchsetzen. Statt dessen setzen sich eher andere Begriffe wie Individualisierung, Personalisierung oder *customization* durch, die jeweils eine Zuschneidung von Angeboten auf Individuen oder Identitäten bezeichnen, für die die Erhebung, Speicherung, Verarbeitung und Nutzung großer Mengen von Informationen über die Individuen oder Identitäten notwendig ist, um die Zuschneidung vornehmen zu können.[1769] Diese Zuschneidung mit ihren Konsequenzen für die Menge der zu verarbeitenden Informationen ist dabei allerdings gar kein neues Phänomen,[1770] auch wenn es in der Diskussion oft als solches behandelt wird. Gleiches gilt für die Profilbildung, mit deren Adressierung der Fokus einerseits auf den Prozess der Profilbildung, andererseits auf das „Halbfertigprodukt“ Profil verschoben wird.[1771] Und gerade die vielen Anwendungsmöglichkeiten von Profilen sind es, die die Erstellbarkeit und Erstellung zum Problemfall machen.[1772] Die dabei problematisierten Anwendungsmöglichkeiten umfassen da-

[1763] Siehe Bellotti und Sellen (1993) für eine der grundlegenden Arbeiten und Roßnagel (2004), Bizer et al. (2006) und Langheinrich (2009) für die nachfolgende Diskussion.

[1764] Der Begriff fand vor allem deshalb Verbreitung, weil die Europäische Kommission Ambient Intelligence als eine der zentralen Visionen im 6. Forschungsrahmenprogramm für den Bereich „Information, Society and Technology (IST)“ aufgriff.

[1765] Neben den Bezeichner „smart objects“ ist inzwischen vor allem „cyber-physical system“ getreten, siehe Broy et al. (2012).

[1766] Siehe Brey (2005), Friedewald und Wright (2006) und Rouvroy (2008).

[1767] Siehe etwa zum Internet of Things Ziegeldorf et al. (2014) und Weber (2015).

[1768] Siehe grundlegend Rost (2004), sowie umfassend Hansen und Meissner (2007, S. 41 ff.). Gleichwohl ist er selbst nicht konsequent und bezeichnet „Verkettbarkeit“ in Rost und Meints (2005, S. 217) als „Verlinkbarkeit“.

[1769] Siehe umfassend Schwenke (2006). Sundar und Marathe (2010) trennt dabei „tailoring“ in „personalization“ und „customization“, wobei ersteres anbieteringesteuert, letztes nutzeringesteuert sei.

[1770] Siehe Arvidsson (2002).

[1771] Gerade in den 1970ern gab es dazu eine umfassende Diskussion, siehe etwa Podlech (1972), Schlink (1973) und insbesondere Benda (1974).

[1772] Siehe Clauß et al. (2005), Rubinstein et al. (2008), Gutwirth und Hildebrandt (2010) und Zarsky (2010) sowie Schermer (2011).

bei sowohl das Scoring,[1773] also das quantifizierende Bewerten von Menschen und vergangenen Ereignissen, „predictive analytics“,[1774] also das Vorhersagen zukünftiger Ereignisse oder zukünftigen Verhaltens, vor allem durch automatisierte Systeme,[1775] *social sorting*,[1776] das Einteilen von Menschen in vordefinierte oder ad-hoc generierte Gruppen, und das dadurch ermöglichte unterschiedliche Behandeln von Menschen, das – insbesondere wenn es zu deren Nachteil geschieht – oft als Diskriminierung bezeichnet wird.[1777] Das Ergebnis dieser fortschreitenden Entwicklungen sowohl im Bereich der Datenverarbeitungmethoden wie der konkreten technischen Systeme, die diese Methoden umsetzen, ist jedenfalls eine wachsende Informations- und daraus folgende Entscheidungsmachtasymmetrie zwischen Datenverarbeiterinnen und Betroffenen zum Nachteil letzteres und mit gesamtgesellschaftlichen Folgen.[1778]

Dass die ganze Debatte enorm begriffsgetrieben geführt wird, zeigt sich etwa daran, dass die gleichen Probleme – von Profilbildung bis Diskriminierung – auch unter dem Label „Big Data“ diskutiert werden.[1779] Vor dem Hintergrund, dass die im Rahmen von Big Data verarbeiteten Daten nie objektiv und oftmals nicht einmal korrekt sind und mehr Daten nicht notwendig die Qualität der Analyse erhöht,[1780] die Algorithmen vorfindliche Verzerrungen in der Datenanalyse schlicht reproduzieren[1781] und darüber hinaus fundierte Analysen vorliegen, die nachweisen, dass selbst jahrzehntealte rechtliche Regelungen wie der Fair Credit Reporting Act von 1970 die aus solchen Verfahren erwachsenden Risiken besser adressieren als alle neueren Regulierungsvorschläge,[1782] überrascht jedenfalls die Selbstverständlichkeit, mit der auf die Vorteile von Big Data verwiesen wird, um eine Änderung zentraler Prinzipien des Datenschutzrechts als erforderlich zu verkaufen.[1783]

2.6.4 Noch mehr „neue“ Theorien

Obwohl zu Anfang des neuen Jahrtausends bereits eine fast unüberschaubare Zahl an *privacy*-, *surveillance*- oder Datenschutztheorien vorlag – auch wenn es oft nur schwer gelingt, die vorgelegten Theorien konzeptionell sauber voneinander trennen zu können –, ist es nicht etwa zu einer Konsolidierung gekommen, sondern eher zu einer fast exzessiven Ausweitung. Neben neuen – oder als „neu“ markierten – und mehr oder weniger grundlegend überarbeiteten Theorien gab es allerdings auch einige Versuche, bestehende Theorien zu ordnen und zu systematisieren sowie miteinander zu vergleichen.[1784]

[1773] Siehe Bizer (2006b) und ULD, GP (2014).
[1774] Siehe etwa Crawford und Schultz (2014) und DeDeo (2015). Anfang der 1970er Jahre wurde das – in einer weniger prozess- als vielmehr systembezogenen Sprache – unter dem Label „Planungsinstrument“ problematisiert, siehe etwa Steinmüller et al. (1971, S. 39 f.).
[1775] Siehe umfassend Pasquale (2015).
[1776] Siehe Dwork und Mulligan (2013). Dazu schon Simitis (1986, S. 29).
[1777] So etwa von Citron und Pasquale (2014) und Zarsky (2014). Ein wesentlicher Anknüpfungspunkt der Debatte ist dabei das Problem der Preisdiskriminierung, siehe beispielhaft Council of Economic Advisers (2015).
[1778] Siehe etwa Newman (2014), Zuboff (2015) und Caplan und boyd (2016).
[1779] Siehe zum Überblick Mayer-Schönberger und Cukier (2013) sowie Tene und Polonetsky (2013).
[1780] Siehe die umfassende Kritik an den Versprechungen der Big-Data-Claqueurinnen etwa bei boyd und Crawford (2011).
[1781] Siehe dazu Barocas und Selbst (2015).
[1782] Siehe Hoofnagle (2013).
[1783] Siehe beispielhaft Kuner et al. (2012) und Tene und Polonetsky (2012).
[1784] Soweit es sich um eine Fortführung einer bestehenden Debatte handelt und auf der theoretischen Ebene keine fundamental neuen Aspekte eingebracht werden, sind die in diesem Zeitraum publizierten Arbeiten bereits in die Darstellung der betreffenden Theorien an entsprechender Stelle eingeflossen.

Mit ihrer Habilitationsschrift „Informationelle Selbstbestimmung“ beabsichtigt Marion Albers, den Datenschutz neu zu konzeptionalisieren.[1785] Sie benutzt dabei einen schon vorher[1786] von Gregory Bateson übernommenen Informationsbegriff, der Informationen als „a difference which makes a difference“ definiert hat.[1787] Im Gegensatz zum Informationsbegriff der Semiotik, der dem Datenschutz historisch zugrunde gelegt wurde, und den sie als Ganzes ignoriert und nur Teile davon – und die auch noch falsch –, kann sie damit nur die syntaktische und die sematische Dimension unterscheiden und endet daher bei einer einfachen Trennung von Daten und Informationen, bei der Informationen mit Sinn versehene Daten sind.[1788] Diese Interpretationsleistung werde dann nur von Menschen erbracht, aber auch das ist falsch, denn es sind soziale Systeme, die diese Leistung erbringen können, und dazu gehören auch Organisationen – und Organisationen sind keine Menschen.[1789]

Albers denkt – und da ist sie keine Ausnahme, eher im Gegenteil – das Problem des Schutzguts von den Informationen her und betrachtet damit die in der Debatte aufgebrachten Regelungsmechanismen nicht als Mittel zu einem Schutzzweck, also als konzeptionell abhängige Variablen, sondern als quasi-selbständige Entitäten,[1790] und arbeitet auf dieser Basis drei Gruppen von Regelungserfordernissen aus der frühen Datenschutzdiskussion heraus: zur „rechtlichen Steuerung der Gewinnung und Umsetzung von Informationen und der Verarbeitung von Daten“, zum „Wissen“ der Betroffenen über „den Umgang mit den sie betreffenden Informationen und Daten“ sowie zu den „Einflußchancen, die den Betroffenen zustehen sollen.“[1791] Aufbauend auf ihrer Analyse und Kritik schlägt sie die Entwicklung von zwei getrennten Schutzregimen – „Ebenen“ – vor.[1792] Das erste Schutzregime soll sich auf die erwartbaren Nachteile von Informations- und Datenverarbeitungen im Lichte konkreter Grundrechte und ihrer Verbürgungen beziehen.[1793] Das zweite Schutzregime soll sich einerseits auf den inhaltlichen Schutzbereich von Art. 2 Abs. 1 GG beziehen, „indem er die Grundrechtsträger in bestimmten Hinsichten in ihrer Identität, ihrer Individualität und in ihrer sozialen Stellung schützt“, andererseit als Vorverlagerung auf abstrak-

[1785] Siehe Albers (2005).

[1786] Siehe Albers (2002).

[1787] Siehe Bateson (1987, S. 321).

[1788] Siehe Albers (2002). So schreibt sie die Veränderung des „Zustandes“ des Empfängers der „Pragmatik“ zu und verweist auf das Datenschutzgutachten, siehe S. 72 und Fn. 49, dabei bezieht sich „Zustand“ gerade auf die „Differenz, die eine Differenz erzeugt“, die sie von Bateson übernimmt, siehe S. 68. Und wenn sie direkt auf den Informationsbegriff, der im Gutachten ausgeführt wird, verweist, dann behauptet sie – ohne den Informationsbegriff selbst zu explizieren, denn sonst würde ihre Argumentation in sich zusammenfallen –, dass dort zwar „die technische Ebene der Datenverarbeitung und die soziale Ebene des Umgangs mit Informationen und Daten“ unterschieden würden, aber „im Ergebnis wird die Differenzierung aber nicht deutlich genug realisiert“, siehe S. 77, Fn. 65.

[1789] Hier liegt wahrscheinlich das zentrale Problem: Albers versucht eine informationelle Selbstbestimmung zu konzeptionalisieren, die sich *gegen alle Dritten* richtet. Das – meist nur implizite, aber im Datenschutzgutachten eben auch explizierte – Angreifermodell der frühen Datenschutzdiskussion zielt aber auf *rationale Verwaltungen*. Aus dieser Differenz ergibt sich notwendig eine sehr unterschiedliche Zuschreibung von Eigenschaften an die Akteurinnen. Die Folgen werden dann in Albers' Kritik deutlich, die mit Begründungen, die sich auf interpersonale Beziehungen beziehen, einen umfassenden Schutzbedarf in vermachteten Beziehungen, etwa zwischen Betroffenen und Organisationen, vor Verhaltenskontrolle und struktureller Beschränkung von Verhaltensspielräumen als zu weit greifend ablehnt, siehe ihre kompakte Darstellung dazu in Albers (2008, S. 122).

[1790] Nicht nur scheint die juristische Arbeitsweise zu einem solchen Umgang einzuladen, sondern gerade auch das Rechtsstaatsprinzip, das einer der wesentlichen Bezugspunkte der Datenschutzdiskussion war, hat sich tatsächlich inzwischen so sehr verselbständigt, dass es fast schon abwegig erscheint, es nur – oder auch nur in erster Linie – als Mittel zur Machtbeschränkung des Staates zu betrachten.

[1791] Siehe Albers (2005, S. 113 ff.).

[1792] Siehe zusammenfassend Albers (2005, S. 589 ff.).

[1793] Siehe dazu schon Garstka (1977) und Gallwas (1979).

tere Risiken „in Konstellationen, in denen bestimmte Folgen zwar zu erwarten, aber noch nicht zu spezifizieren oder abzuschätzen sind oder in denen eine Bündelung vielfältiger Situationen und Folgen notwendig ist."[1794]

In den letzten Jahren ist ein Topos wieder stärker in den Vordergrund gerückt, der schon im Zuge der Diskussion in den 1960ern, vor allem aber im Umfeld von Podlech und Steinmüller problematisiert wurde: die Tendenz automationsgestützter Entscheidungssysteme, Verfahrensgarantien strukturell zu untergraben und dabei Beteiligungsrechte und -möglichkeiten der Betroffenen zu beschränken, indem die ihnen eingebauten Regeln an die Stelle der Rechtsregeln treten, sowie die Tendenz von Betreiberinnen solcher Systeme, die Systemprodukte für wahr zu halten, weil sie von den Systemen erzeugt werden.[1795] Während Steinbock explizit Bezug auf die *privacy*-Debatte nimmt und sie für das von ihm analysierte Problem für zu kurz greifend hält, kommen sowohl Citrons Analyse wie auch ihr Lösungsvorschlag ohne jede Bezugnahme auf Vorarbeiten aus der *privacy*- und Datenschutzdiskussion aus, weder aus der historischen noch aus der zeitgenössischen. Auch die von Citron zusammen mit Frank Pasquale vorgenommene Übertragung dieses Analyseansatzes auf automationsgestützte Scoringsysteme bleibt dafür blind, obwohl sie ihren Regulierungsvorschlag in Anlehnung an den Fair Credit Reporting Act of 1970 entwickeln.[1796] Auf der anderen Seite des Atlantiks versuchen Paul de Hert und Serge Gutwirth, *privacy* und Datenschutz genau an dieser Stelle konzeptionell zu trennen: *Privacy* identifizieren sie dabei als „tool of opacity", das dazu diene, der Macht normative Grenzen zu setzen und sie zu stoppen, während Datenschutz vor allem ein „tool of transparency" sei, mit dem legitime Machtausübung eingehegt und kanalisiert werde.[1797] Dabei solle *privacy* vor der Einmischung des Staates und privater Akteurinnen in die Autonomiebereiche der Individuen schützen, während Datenschutz vor allem darauf ziele, mittels prozeduraler Sicherungsmechanismen die *privacy* des Individuums zu schützen und eine Rechenschaftspflichtigkeit von staatlichen und privaten Datenverarbeiterinnen zu erzeugen.[1798] An diese Diskussion knüpfen Mireille Hildebrandt und Katja de Vries mit einem Sammelband an, in dem etwa Antoinette Rouvroy (wieder-)entdeckt, dass allen propagandistischen Behauptungen, nach denen Menschen und ihre Situationen und Bedürfnisse, ihre Fähigkeiten und Präferenzen in den Mittelpunkt gestellt würden, zum Trotz das automatisiert generierte Profil den Menschen als Bezugspunkt ersetzt, und Bert-Jaap Koops die alte Doppelstrategie des Datenschutzes, die sich nur in verkürzter Form im Datenschutzrecht wiederfindet, wieder neu als Lösung vorschlägt: Nicht die Betroffenen sollen

[1794] Siehe Albers (2005, S. 594).

[1795] Siehe mit Bezug ausschließlich auf den öffentlichen Bereich Steinbock (2005) sowie allgemein Citron (2008). Daniel J. Steinbock spricht dabei ganz allgemein von „due process", während Danielle Keats Citron einen neuen Begriff schafft: „technological due process". Und Crawford und Schultz (2014) nennen das dann sogar „procedural data due process".

[1796] Siehe Citron und Pasquale (2014). Einer der zentralen Kritikpunkte von Zarsky (2014, S. 1378 f.), adressiert genau diese Leerstelle und verweist dabei auf die Genese des Codes of Fair Information Practice.

[1797] Siehe De Hert und Gutwirth (2006). *Opacity* soll dabei nicht auf Unsichtbarkeit hinweisen, sondern auf Nichteinmischung, siehe S. 67, Fn. 16, während *transparency* als Pars pro Toto für das Rechtsstaatsprinzip stehen soll, siehe S. 69 f.

[1798] Siehe De Hert und Gutwirth (2006, S. 71, 77 f.), wobei sie zugleich die Prozeduralisierung des Rechts an dieser Stelle kritisieren, weil sie zu Formalisierung, Bürokratisierung und Depolitisierung führe und im Zuge dessen formelle Bedingungen und Beschränkungen erzeugt würden, die eine inhaltliche Prüfung ersetzten und niemals so hoch seien, dass sie nicht erfüllt werden könnten, siehe S. 87 ff. Gutwirth wird später zwischen einem instrumentellen Verständnis, in dem Datenschutz dem Schutz *aller* Grundrechte, auch *privacy*, dient, auf der einen und einem Verständnis von gegenseitiger Unabhängigkeit unterscheiden, siehe Gellert und Gutwirth (2013). Lisa M. Austin hingegen will die Trennung absolut machen und die Verbindung zwischen Datenschutz und *privacy* ganz kappen, siehe Austin (2014) und vor allem Austin (2015).

von den Organisationen transparent gemacht werden können, sondern den Betroffenen sollen die Datenverarbeiterinnen, ihre Informationsverarbeitungs- und Entscheidungsfindungsprozesse sowie die Entscheidungen selbst transparent gemacht werden.[1799]

In dem Teil der Debatte, der *privacy* als Bezugspunkt ansieht, scheint Kate Raynes-Goldie die erste zu sein, die in ihren Arbeiten sauber zwischen den Geltungsbereichen von Theorien zu trennen versucht.[1800] Sie unterscheidet dabei zwischen *social privacy* und *institutional privacy*, wobei *social privacy* sich auf „the management of what is disclosed about oneself to others (also called identity or reputation management) and the ability to navigate and manage various social contexts" beziehe und *institutional privacy* darauf, „how institutions such as governments, banks and other businesses, use or misuse their personal information".[1801] Zwei Probleme sind jedoch nicht zu übersehen: Erstens ist ihre Analyse der *privacy*-Debatte total verkürzt, indem sie unterstellt, die Debatte kreise bislang fast ausschließlich um *institutional privacy*, obwohl eher das Gegenteil der Fall ist, unter anderem weil sie fast die gesamte auf Goffman und Altman aufbauende Diskussion ignoriert. Und zweitens sind die beiden Geltungsbereiche nicht überschneidungsfrei – ganz im Gegenteil. Das liegt daran, dass sie die Bereiche nach zwei fundamental unterschiedlichen Kategorien trennt – *institutional privacy* wird durch die Auswahl an Datenverarbeiterinnen konstituiert, die betrachtet werden, während *social privacy* durch individuelle Praktiken der Betroffenen bestimmt wird. Diese Trennung ist damit strukturell blind für Situationen, in denen die Praktiken, die unter *social privacy* gefasst werden, gegenüber Organisationen eingesetzt oder gerade von Organisationen verhindert werden.

Titus Stahl analysiert die Folgen der Massenüberwachung durch Geheimdienste in einer Weise, die an Rosts Datenschutztheorie erinnert, allerdings nur unter Verweis auf Habermas – und nicht auch Luhmann –, nur für die Sphäre der politischen Öffentlichkeit – und nicht für alle gesellschaftlichen Subsysteme – und eben beschränkt auf die Massenüberwachung – und nicht bezogen auf moderne Organisationen und deren Informationsgebaren insgesamt.[1802] Stahl stellt fest, wie vor ihm schon Roßnagel für soziotechnische Informationssysteme im Allgemeinen, dass „[n]ew technologies of indiscriminate mass surveillance [...] shape the public sphere in a way that is likely to have an effect on those reasons that are dependent on the citizens standing in certain kinds of relationships in the public sphere" – oder in Roßnagels Worten: sie beeinflussen die „Verwirklichungsbedingungen für Verfassungsziele".[1803] Mit Habermas schlussfolgert er dann, dass „surveillance of the public sphere undermines the specific form of rationality that this sphere displays in the ideal case" und „surveillance must count as an intervention into the process of collective reasoning distinctive to this sphere."[1804]

In den letzten Jahren wurden einige Arbeiten publiziert, deren primäres Interesse darin bestand, die bestehenden Theorien – oder zumindest eine Auswahl davon – zu ordnen und zu systematisieren sowie miteinander zu vergleichen oder – wie schon Rule und Kolleginnen 1980,

[1799] Siehe Hildebrandt und de Vries (2013) sowie Rouvroy (2013) und Koops (2013). Die Ersetzung der Menschen durch ihre Profile und deren Verselbständigung hat schon Anér (1972, S. 179) unter dem Begriff „data-shadow" problematisiert.

[1800] Siehe Raynes-Goldie (2010) und die umfassendere Dissertation, Raynes-Goldie (2012).

[1801] Siehe Raynes-Goldie (2012, S. 81, 80).

[1802] Siehe Rost (2014a, S. 41, Nr. 7): „Die gesellschaftliche Funktion des Datenschutzes besteht darin, die Risikoquellen der funktionalen Differenzierung – Markt, Demokratie und Gewaltenteilung sowie freie wissenschaftliche, ästhetische und religiöse Diskurse – gegen die latenten Angriffe der Organisationen zu bewahren oder zu stärken."

[1803] Siehe Stahl (2016, S. 36) und Roßnagel (1989a, S. 143). Siehe auch die umfassende – und technisch wohlinformierte – Darstellung bei Caplan und boyd (2016).

[1804] Siehe Stahl (2016, S. 37).

Clarke Mitte der 1990er Jahre oder Kang Ende der 1990er Jahre[1805] – Schutzgüter oder Schutzregime zu typisieren.[1806]

Herman Tavani unterscheidet vier Arten von *privacy* – *physical* oder *accessibility privacy*, *decisional privacy*, *psychological* oder *mental privacy* sowie *informational privacy* – und glaubt, dass es drei „full-fledged" *privacy*-Theorien – die „Restricted Access Theory" nach Gavison, die „Control Theory" nach Westin und die „Restricted Access/Limited Control Theory", die er selbst vertritt, – und drei Theorieskizzen – „Privacy as Contextual Integrity" nach Nissenbaum, Floridis „Ontological Interpretation" und Vedders „Categorical Privacy". Darüber hinaus will er *informational privacy* jeweils nach „aspects of an individual's life", die betroffen seien, unterscheiden und liefert als Beispiele für seine „categories of informational privacy" *consumer privacy*, *medical privacy*, *employee privacy* und *location privacy*.[1807] Thomas Allmer behauptet, eine Systematisierung der *privacy*-Theorien vorzunehmen, indem er sie als individualistische, strukturalistische und integrative Theorien identifiziert.[1808] Stephen Margulis behauptet, in seiner Arbeit „the current most important theories of privacy" darzustellen, und wählt dann Alan Westins, Irwin Altmans und Sandra Petronios Theorien aus. Die ersten beiden bezeichnet er als „the two best articulated and best supported" *privacy*-Theorien, Petronios als „an important extension" von Altmans Theorie sowie als „[t]he most valuable privacy theory for understanding interpersonal computer-mediated communication".[1809] Jeff Smith und Kolleginnen klassifizieren *information privacy*-Theorien in zwei Dimensionen: danach, ob sie normativ, rein deskriptiv oder empirisch deskriptiv sind, und danach, ob sie sich auf die individuelle, Gruppen-, Organisations- oder die gesellschaftliche Ebene beziehen.[1810] *Privacy*-Theorien werden entweder als auf (absoluten) Werten oder auf individuellen Vorstellungen basierend angesehen, wobei erste wieder unterteilt werden in *privacy as right* und *as commodity*, letztere in zustandsbasierte und kontrollbasierte Theorien.[1811] In Abgrenzung zu benachbarten Konzepten stellen sie fest, dass Anonymität, Geheimhaltung, Vertraulichkeit, Sicherheit und Ethik nicht das gleiche seien wie *privacy*.[1812] Carsten Ochs und Petra Ilyes untersuchen die Forschungslandschaft im Umfeld der

[1805] Siehe Rule et al. (1980, S. 47), Clarke (1995) und Kang (1998, S. 1202 ff.).

[1806] Die hier vorgenommene Beschränkung auf Arbeiten mit einem primären Interesse an der Typisierung und Systematisierung existierender Ansätze folgt schlicht aus der Tatsache, dass die vorliegende Arbeit weder das Ziel verfolgt, *alle* jemals vorgenommenen Typisierungen und Systematisierungen darzustellen, noch dem Glauben anhängt, dass sich aus Typisierungen und Systematisierungen von teilweise offensichtlich arbiträr ausgewählten Theorien und auf der Basis von teilweise ebenso arbiträr konstruierten Kategorien besonders viele Erkenntnisse gewinnen ließen.

[1807] Siehe Tavani (2008). Die Auswahl der Theorien wird nicht begründet, insbesondere nicht hinsichtlich der Theorieskizzen. Die „Control Theory" wird darüber hinaus falsch dargestellt, siehe S. 143 zur Art der Informationen, auf die sich die Theorie bezieht. Darüber hinaus ist die Unterscheidung zwischen der „Restricted Access Theory" und der „Control Theory" artifiziell: Erstere beschreibt *privacy* als Zustand der Beschränkung des Zugriffs Dritter auf Informationen, letztere als Kontrolle, wer Zugriff auf die Informationen hat.

[1808] Siehe Allmer (2011). Seine Einordnung ist absurd unwissenschaftlich, schon weil er alle Theorien, die *privacy* als „moral or legal right" bezeichnen oder durch das Recht geschützt sehen wollen, als strukturalistisch markiert, siehe S. 85.

[1809] Siehe Margulis (2011, S. 9, 12). Obwohl er das sogar explizit anschneidet, scheint Margulis das Problem des Geltungsbereichs nicht zu verstehen, wenn er behauptet, die von ihm betrachteten Theorien würden untersuchen, „how individuals and groups control or regulate access to themselves" (S. 15), obwohl Altmans Theorie dieses Verhalten *nur* gegenüber anderen Individuen und Gruppen abdeckt.

[1810] Siehe Smith et al. (2011). Zentrales Ziel der Arbeit ist zu untersuchen, wie sich „new insights in the IS domain" generieren lassen, und vertritt dabei deutlich eine positivistische Position, siehe S. 1006, und dieses Ziel bedingt deutlich die Auswahl der untersuchten Literatur, die vor allem aus empirischen Arbeiten besteht, und ihre Analyse.

[1811] Smith et al. (2011, S. 992 ff.).

[1812] Smith et al. (2011, S. 995 f.).

Science and Technology Studies zu *information privacy*, die sie *sociotechnical privacy* nennen, und klassifizieren diese als quantitative und qualitative Untersuchungen.[1813] Rachel Finn und Kollegen unterscheiden sieben Typen von *privacy*: „privacy of the person" als das Recht, „to keep body functions and body characteristics (such as genetic codes and biometrics) private", „privacy of behavior and action" als innere und äußere Entscheidungs- sowie Handlungsfreiheit, „privacy of communication" als Vertraulichkeit der direkten und der technisch vermittelten Kommunikation und ihrer Umstände, „privacy of data and image", „privacy of thoughts and feelings", „privacy of location and space" einschließlich des Rechts, sich anonym, unbeobachtet und unverfolgt in der Öffentlichkeit zu bewegen, sowie „privacy of association", die auch „group privacy" beinhalte.[1814] Stefan Drackert versucht, aus der *deutschen und europäischen* Rechtsprechung und willkürlich ausgewählter, fast ausschließlich *deutscher* Literatur Schutzgüter und Risiken zu destillieren, die das *deutsche* Datenschutzrecht prägen, dass die Schutzgüter vor den Risiken zu schützen versucht.[1815] Die von ihm identifizierten Risiken klassifiziert er nach strukturellen Risiken auf der Makroebene, überwiegend individuellen Risiken auf der Mikroeben und Risiken für Gesellschaft und Individuum auf der Makro- und Mikroebene, und schließt sogenannte Grenzfälle und Nicht-Risiken aus – unter anderem einen Großteil der Datenverarbeitung durch die Privatwirtschaft wie Werbung und Zielgruppenpräzisierung etwa durch „behavioral tracking" oder Bonitätsprüfungen und Forderungsmanagement.[1816] Kai von Lewinski ordnet die

[1813] Siehe Ochs und Ilyes (2013). Zwar übernehmen sie von Raynes-Goldie die Trennung in *institutional privacy* und *social privacy*, siehe S. 79, aber nutzen das nicht, um die von ihnen beschriebenen Arbeiten einzuordnen. Und für eine Forschungsrichtung wie die Science and Technology Studies ist es schon relativ peinlich, dass wichtige Arbeiten aus einer der Basisdisziplinen – Soziologie – komplett ignoriert werden, etwa die Arbeiten von James Rule und Kolleginnen oder Paul Müller, während Hannah Arendt als Soziologin verkauft wird, siehe S. 74.

[1814] Siehe Finn et al. (2013). Die Abgrenzung zwischen den Typen gelingt den Autorinnen nur bedingt. So bleibt etwa unklar, warum die „sexual preferences" als Teil der „privacy of behavior and action" gelten, wenn es eine weitere Kategorie gibt, die „thoughts and feelings" adressiert, siehe S. 8 f., denn die gelieferte Begründung, dass Gedanken nicht automatisch in Verhalten münden, gilt für sexuelle Präferenzen ja gerade auch. Genauso unklar ist, warum personenbezogene Informationen über das Bewegen in der Öffentlichkeit zu „privacy of location and space" gehören sollen, nicht jedoch zu „privacy of data and image".

[1815] Siehe Drackert (2014). Die Willkür zeigt sich in erster Linie darin, welche Arbeiten er schlicht unterschlagen hat: *fast alle, die nicht von einem individualistischen Standpunkt aus Befindlichkeiten zu Schutzgütern erklären.* Dazu gehörden die Arbeiten von Ulrich Seidel, Christoph Mallmann, Paul Müller, Ulrich Dammann, Eggert Schwan (der zumindest an einer Stelle vermittelt zitiert wird, siehe S. 281, Fn. 16) und Bernhard Schlink, von Podlech betrachtet er nur eine Arbeit und von Steinmüller abgesehen vom 1971er Datenschutzgutachten keine Arbeiten aus den 1970ern. Hinzu kommen die – wenigen – „Begründungen" für seine Auswahl, die teilweise offenkundig falsch sind – „werden jedoch dem Stand der technischen und gesellschaftlichen Entwicklung nicht mehr gerecht" (und das von einem Juristen, dem es offenkundig an informatischen und soziologischen Kenntnissen mangelt), „eine grundsätzlich misstrauische oder sogar ablehnende Haltung gegenüber moderner Informationstechnologie" oder „[d]erartige postmarxistische Begründungsansätze sind ideologisch geprägt und können nicht überzeugen", siehe S. 9 f. – und das gerade vor dem Hintergrund seiner eigenen, ideologisch geprägten Begründungen, siehe etwa S. 282. Und nicht zuletzt ist auch die Auswahl der in seine Analyse einbezogenen Arbeiten mehr als fragwürdig, etwa wenn er die 1977 veröffentlichte „grundlegende[]" Arbeit Otto Mallmanns einbezieht wegen „ihrer soziologischen Bezüge und rechtspolitischen Ausrichtung", siehe S. 9, obwohl sie eine nur unwesentlich erweiterte Fassung von Westins Arbeit ist, fast keinen Einfluss auf die Datenschutzgesetzgebung hatte und auch nicht soziologisch, sondern sozialpsychologisch argumentierte, während er Christoph Mallmanns tatsächlich soziologische Bezüge beinhaltende Arbeit ignoriert.

[1816] Siehe zu letzterem Drackert (2014, S. 311 ff.). Er hält es – trotz seiner vorherigen Bezugnahme auf überindividuelle und gesellschaftliche Aspekte – für ausreichend zu bezweifeln, dass damit „tatsächlich rechtspolitisch zu missbilligende individuelle Nachteile einhergehen", siehe S. 312, und erklärt die Verteuerung oder das Nichtzustandekommen von Verträgen aufgrund der Verarbeitung personenbezogener Informationen sei kein „datenverarbeitungsrechtliches Risiko, sondern [...] ein allgemeines Lebensrisiko", siehe S. 314. Sowohl seine Explikation von bestimmten Risiken und deren Zuordnung zur Mikro-, Makro- und zur Mikro-/Makroebene ist extrem

auf Deutsch unter dem Label „Datenschutz“ diskutierten Schutzgüter und Schutzkonzepte in eine zweidimensionale Matrix ein, bei der die Schutzgüter nach ihrem Abstraktionsgrad aufsteigend geordnet sind und zugleich eine „Vorfeldschutz-Kaskade“ – mit Rückkopplung von der gesamtgesellschaftlichen zurück auf die individuelle Ebene – abbilden, und bei der die Schutzkonzepte eingeteilt sind in außerrechtliche Schutzansätze, direkt wirkende normative Schutzregeln und Vorfeldschutzmechanismen.[1817] Die Kaskade der Schutzgüter beginnt mit dem „innere[n] Kern des Menschseins“, seinem „Eigenwert“, gefolgt von räumlichen, sozialen oder „logischen“ – informationstechnischen – Herrschaftsbereichen, dem als „informationelle Fremdbeschränkung“ bezeichneten Abwehraspekt des sonst „informationelle Selbstbestimmung“ genannten Schutzguts, einer auch als „market privacy“ bezeichneten informationellen Verfügung und endet beim „gesellschaftliche[n] Informationsgleichgewicht“, das dann aber wieder auf den Einzelnen zurückwirke.[1818] Und zuletzt haben Bert-Jaap Koops und Kolleginnen eine *privacy*-Typologie vorgelegt, die auf der Basis einer Analyse des verfassungsrechtlichen *privacy*-Schutzes in neun Ländern – USA, Canada, UK, die Niederlande, die Bundesrepublik, Italien, Tschechien, Polen und Slowenien – sowie der zugehörigen wissenschaftlichen Literatur acht Typen in zwei Dimensionen – Ausrichtung auf „Freiheit von“ („being let alone“) und auf „Freiheit zu“ („self-development“) – ableiten mit einer neunten, alle anderen Typen überschneidenden, aber nicht mit ihnen übereinstimmenden *privacy*: der *informational privacy*.[1819] Die acht nicht-informationellen Typen sind jeweils auf einer Achse von einer „personal zone“ über eine „intimate zone“ und eine „semi-private zone“ bis zu einer „public zone“ eingeordnet – mit der Ausrichtung auf „Freiheit von“ sind das „bodily privacy“, „spatial privacy“, „communicational privacy“ und „proprietary privacy“ und mit der Ausrichtung auf „Freiheit zu“ „intellectual privacy“, „decisional privacy“, „associational privacy“ und „behavioral privacy“.[1820]

2.6.5 Privacy by Design

In den letzten 10 bis 15 Jahren wurden viele Vorschläge mit neuem Namen vorgelegt, darunter waren aber nicht unbedingt genauso viele neue Ansätze. Teilweise werden explizit ältere Ansätze wie KORA weitergenutzt[1821] – auch wenn nicht klar ist, ob sie auch weiterentwickelt werden –, teilweise sind die Konzepte auch einfach nur durch eine extreme Ähnlichkeit zueinander geprägt. Vor allem die Erzeugung von Anonymität nimmt weiterhin einen breiten Raum ein. In den

defizitär: Die Nichtharmonisierung des Datenschutzrechts als Risiko, das das Datenschutzrecht adressiere, zu identifizieren, siehe S. 288 ff., ist selbst für einen Juristen lächerlich, problematischer ist, dass die Risiken auf ganz unterschiedlichen Abstraktionsstufen – von direkten Auswirkungen wie Diskriminierung bis zu abstrakten Risiken wie „Informationspermanenz“ – liegen, ohne dass Drackert das reflektiert.

[1817] Siehe von Lewinski (2014).

[1818] Siehe von Lewinski (2014, S. 17 ff.,82 f.). Der gewählte Startpunkt in der Kaskadenstruktur ergibt sich aus der klassisch liberalistisch und damit individualistisch geprägten Ordnung der *Grundrechte*, siehe S. 17 f., nicht aber – wie von Lewinski richtig feststellt – aus der Geschichte der Normierung des Datenschutzes, siehe S. 82. Aus strukturalistischer Sicht und gerade vor dem Hintergrund der Genese des Datenschutzes als Mittel zur Informationsmachtbeschränkung – und den zentralen Staatsorganisationsprinzipien als der zweiten Säule des Datenschutzrechts – steht noch aus, die Kaskadenstruktur vom Kopf auf die Füße zu stellen.

[1819] Siehe Koops et al. (2016).

[1820] Siehe Koops et al. (2016, S. 66 ff.). Abgesehen von den von den Autorinnen selbst schon kritisch angemerkten Punkten, siehe S. 73 ff., stellt sich die Typologie deutlich als Reproduktion der Sphärentheorie dar, in der einer der zentralen Aspekte der Datenschutzdebatte komplett ausgeblendet wird – oder zwischen den Typen einfach „verschwindet“: die Sicherung von Verhaltensfreiheit gegenüber informationsmächtigen Akteurinnen, die mittels ihrer Informationsmacht in der Lage sind, die Verwirklichungsbedingungen dieser Freiheit strategisch zu Ungunsten der schwächeren Akteurin zu beeinflussen.

[1821] Siehe etwa Bräunlich et al. (2011) und Hoffmann et al. (2011).

einzelnen Vorschlägen für Methoden der Ableitung von konkreten technischen Anforderungen aus allgemeinen oder abstrakten *privacy*- oder Datenschutzanforderungen, die dann von Technik erfüllt werden sollen, wird nicht immer deutlich gemacht, woher die Anforderungen stammen, die dort jeweils zur Grundlage gemacht werden – in Teilen sind sie wohl auch einfach aus der Luft gegriffen. Vermehrt werden auch die existierenden Vorschläge selbst zum Gegenstand von Untersuchungen gemacht, vor allem in vergleichenden Arbeiten.[1822]

Die sich bereits in den 1990er Jahren abzeichnende und ab Beginn des neuen Jahrtausends verstärkende Verschiebung der Debatte zur den Entwicklungsmethoden von Systemen, die von Organisationen zur Verarbeitung von Informationen über Menschen eingesetzt werden, hin zu solchen, die von den Betroffenen (auch) selbst eingesetzt werden oder mit denen sie interagieren, hat zugleich zu einer Verschiebung des Fokus bei den Bedrohungsanalysen geführt: Während – abgesehen von den wenigen „klassischen" datenschutzorientierten Gestaltungsansätzen[1823] – schon früher wegen eines auf Personen fixierten Verständnisses von *privacy*-Bedrohungen die Analysen eher weniger auf die informationsverarbeitenden Organisationen, sondern vor allem auf deren Mitarbeiterinnen sowie externe Angreiferinnen fokussierten, ist die Organisation im Verlauf der Diskussion immer weiter aus dem Blickfeld der Bedrohungsanalysen verschwunden oder gar zur Verteidigerin der *privacy* der Betroffenen mutiert.[1824] In der Folge stellen sich viele aus den Analysen abgeleitete Anforderungen an die Systemgestaltung aus Datenschutzsicht als deutlich bruchstückhaft heraus, die selbst erst wieder in passender Form als Bausteine in ein umfassenderes System von Entwicklungsmethoden und Systemanforderungen eingeordnet werden müssen.

Solche Bausteine sind etwa die von Scott Lederer et al. – beschränkt auf Aspekte, die sich aus Altmans interpersonaler *privacy*-Theorie zur Praxis des Changierens zwischen *disclosure* und *non-disclosure* – identifizierten Gestaltungsanforderungen für Endnutzerinnensysteme:[1825] Entwicklerinnen sollen sowohl die potentiellen wie die tatsächlich stattfindenden Informationsflüsse den Nutzerinnen transparent machen; Systeme sollten – eine frühe Form von *Privacy by Default*, vielleicht die erste – keiner exzessiven Vorkonfiguration bedürfen, um Nutzerinnen das Management ihrer *privacy* zu ermöglichen; Systeme sollten direkt auf dem zentralen User Interface grobkörnige Kontrollmechanismen mitbringen, von An-/Aus-Schaltern bis zu Genauigkeitseinstellungen für Ortsinformationen; und Systeme sollten sich an etablierte soziale Praktiken im Umgang mit *privacy* halten und sie nicht unterlaufen. Soziale Praktiken sind aber nicht statisch, nicht im Beziehungen zwischen Menschen, aber auch nicht innerhalb von Organisationen, mehr noch: insofern Entscheidungen gerade „Absorption von Unsicherheit"[1826] sind, müssen Entscheidungsspielräume – oder allgemeiner: Kontingenzen – offenbleiben, die dann aber auch

[1822] Siehe dazu etwa die Auseinandersetzung mit und zwischen den verschiedenen Requirements-Engineering-Methoden, Ziele – „goals", also Organisations- und Geschäftsziele sowie Gestaltungs-, Entwicklungs- und Sicherheitsziele – und deren Verhältnisse zueinander einschließlich ihrer Widersprüche als funktionale und nicht-funktionale Anforderungen zu modellieren, um erstens zwischen ihnen abwägen zu können und zweitens Systeme so zu gestalten, dass sie diese Ziele erreichen können, Kalloniatis et al. (2004), Kavakli (2004), Kavakli und Loucopoulos (2005) und Lapouchnian (2005), sowie vergleichbare Arbeiten zum Security Requirements Engineering, Elahi (2008) und Fabian et al. (2010).

[1823] Also etwa Steinmüller et al. (1978), Bräutigam et al. (1990) oder Hammer et al. (1992).

[1824] Siehe etwa die Ausführungen bei Hong et al. (2004, S. 3 und 5). Siehe auch Brodie et al. (2005, S. 35): Die Organisation wird nur noch in ihrer Fähigkeit „to protect that information and enforce privacy policies" betrachtet, während die betrachteten Bedrohungen sich beschränken auf „external break-ins as well as accidental and malicious misuse of personal information by individuals within an organization".

[1825] Siehe Lederer et al. (2004).

[1826] Siehe grundlegend schon Luhmann (1966a, S. 56 f.).

modellierbar sein müssen, auch um im Technikentwicklungsprozess verhandelbar, mit anderen Zielen abwägbar und in der Technik am Ende umsetzbar zu sein. Einen Ansatz, um „bewusste Auslassungen [...], erkannte Unvollständigkeiten und [...] situative[] Entscheidungen“, aber auch Perspektivenvielfalt und selbstreferenzielle Änderungen des Systems abbilden zu können, präsentieren vor diesem Hintergrund Thomas Herrmann et al. mit der Methode des „sociotechnical walkthrough“ und der Modellierungssprache SeeMe.[1827] Und Paolo Giorgini et al. erweitern die Methode Secure Tropos um die Abbildbarkeit von Vertrauens- und Abhängigkeitsbeziehungen zwischen sozialen Akteurinnen,[1828] mit der dann Fabio Massacci et al. versuchen, die Informationsverarbeitung der Universität Trient gemäß dem Italienischen Datenschutzgesetz abzubilden,[1829] und die später von Luca Compagna et al. in „security and privacy patterns“ überführt werden.[1830]

Das konzeptionelle Gegenteil zu Herrmann et al. verfolgt eine Gruppe um Annie Antón: Während erstere Mehrdeutigkeiten und Kontingenzen aufrechtzuerhalten versucht, legt letztere eine Methode vor, die bei der Übersetzung von rechtlichen in technische Anforderungen alle Mehrdeutigkeiten auflösen soll, dabei allerdings Abwägungsanforderungen komplett ausblendet und damit einen Umgang mit rechtlich gebotenen Abwägungen zwischen jeweils legitimen Interessen nicht erlaubt.[1831] Und das konzeptionelle Gegenstück zu Massacci et al. kommt aus den Feder von Christos Kalloniatis et al., die erst vier und später acht *privacy requirements* identifizieren und in Pattern umsetzen, denn das Datenschutz-Pattern – die anderen sieben sind Identifizierung, Authentifizierung, Authentisierung, Anonymität, Pseudonymität, Unverkettbarkeit und Unbeobachtbarkeit – lautet schlicht: „if the user asks to perform any of the above tasks the system checks whether this complies with the privacy regulation and the request is either granted or denied, accordingly.“[1832]

Spiekermann und Cranor unterscheiden drei Kontrollsphären – die „user sphere“, die „recipient sphere“ und die „joint sphere“ –, die entweder allein von den Nutzerinnen, allein von den Datenverarbeiterinnen oder von beiden gemeinsam kontrolliert werden, sowie drei Funktionen von Systemen – „data transfer“, „data storage“ und „data processing“, wobei letzteres sowohl „use“ wie auch „transformation“ umfasst –, auf die sie in der Folge aber schlicht nicht mehr Bezug

[1827] Siehe zur Übersicht Hermann et al. (2004). Siehe für eine umfassendere, mit den theoretischen Hintergründen und Fallanalysen unterfütterte Analyse Herrmann et al. (2004) sowie zur Modellierungsnotation Herrmann (2006).

[1828] Siehe Giorgini et al. (2004), Giorgini et al. (2005) und Giorgini et al. (2006). Abhängigkeit meint hier unter anderem Abhängigkeit bei der Erreichung von Zielen, der Erfüllung von Aufgaben etc.

[1829] Siehe Massacci et al. (2004).

[1830] Siehe Compagna et al. (2007) und Compagna et al. (2009). In allen drei Fällen handelt es sich um die gleiche Arbeitsgruppe unter der Leitung von Fabio Massacci. Die in den zitierten Arbeiten vorgestellten Tools wurden nach Angaben auf den Webseiten, auf die in den Papers verwiesen wird, seit mindestens 2011 nicht mehr weiterentwickelt. Diese Beobachtung lässt sich auf sehr viele dieser Projekte übertragen: Methoden, aber auch Tools werden entwickelt, es gibt ein paar Veröffentlichungen, und dann schläft das Projekt wieder ein, die Webseiten verschwinden und mit ihnen die entwickelten Tools. Siehe etwa Harbird et al. (2008) für ein Werkzeug zur Unterstützung von PIAs, dem das gleiche Schicksal passierte.

[1831] Siehe Breaux und Antón (2005), Breaux und Antón (2007) und Massey et al. (2010). Der ganze Vorschlag scheint vor allem deshalb sehr „beschränkt“ zu sein, weil er in starker Anlehnung an den HIPAA entwickelt wurde, der solche Abwägungsanforderungen nicht enthält. Dies legt jedenfalls auch ein anderer Vorschlag nahe, siehe Siena et al. (2009), der die gleiche Beschränkung aufweist und auch nur HIPAA betrachtet. Siehe zur Kritik an solchen beschränkten Ansätzen, vor allem am Beispiel der EG-Datenschutzrichtlinie, Kiyavitskaya et al. (2008).

[1832] Kalloniatis et al. (2007, S. 1011). Siehe grundlegend Kalloniatis et al. (2005) und Kavakli et al. (2006).

nehmen.[1833] Auf der Basis einer – sehr überspritzten – Unterscheidung zwischen „[c]ryptography researchers and privacy rights organizations“, die eine Verarbeitung personenbezogener Informationen unter allen Umständen verhindern wollen, und den Akteurinnen, die „acknowledge that information may be collected for useful purposes such as personalized services“, schlagen sie dafür zwei ebenso überspritzt konstruierte Systemgestaltungsansätze vor: „privacy-by-policy“ und „privacy-by-architecture“, wobei der erste Ansatz das Ziel verfolgt, einer Datenverarbeiterin dabei zu helfen, „to implement just enough privacy mechanisms to let users feel comfortable and perceive an adequate level of protection [...] providing users with some degree of control over their personal data“, der zweite hingegen auf Anonymität, mindestens jedoch auf Datenminimierung zielt.[1834] Seda Gürses und Jose del Alamo stellen diesen zwei Ansätzen später einen dritten zur Seite – „privacy by interaction“.[1835] Sie ordnen dabei „privacy-by-policy“ das Ziel zu, Organisationen und deren Informationsverarbeitung zu adressieren, während „privacy-by-architecture“ auf die Verhinderung von „unintended inferences“ ziele – es stellt sich die Frage, von wem – und „privacy by interaction“ *privacy*-Probleme adressiere, „that arise, for example, between peers or in a workplace due to the introduction of information systems.“[1836]

Einen völlig anderen Ansatz verfolgen Rost und Pfitzmann, indem sie die drei traditionellen Schutzziele der IT-Sicherheit – Vertraulichkeit, Verfügbarkeit und Integrität – um drei explizit auf Datenschutz orientierte Schutzziele – Transparenz, Unverkettbarkeit und Kontingenz, wobei die letzten beiden später Nichtverkettbarkeit und Intervenierbarkeit genannt werden –, die zwischen den Bereichen Recht, Organisation und Technik vermitteln helfen, ohne dass die Eigenlogik eines der Bereiche die Eigenlogiken der anderen Bereiche dominiert.[1837] Dabei werden die Schutzziele zugleich systematisiert, indem jeweils zwei einander als Duale gegenübergestellt werden, also einem in Bezug auf eine Referenz widersprüchlichen, jedoch in Bezug auf verschiedene Referenzen einander ergänzenden Verhältnis: Verfügbarkeit als Dual zu Vertraulichkeit, Transparenz als Dual zu Nichtverkettbarkeit und Integrität als Dual zu Intervenierbarkeit.[1838] Zugleich lassen sie die Schutzziele auf alle drei Komponenten eines Verfahrens – oder *use cases* oder Geschäftsprozesses – anwenden, auf Informationen, Systeme und Prozesse.[1839] Auf der Basis der sechs Schutzziele, der drei Verfahrenskomponenten sowie von drei Schutzstufen – normal, hoch

[1833] Siehe Spiekermann und Cranor (2009, S. 68 ff.). Die „joint sphere“ ist allerdings, wie die Autorinnen korrekt feststellen, eine von den Datenverarbeiterinnen *allein* kontrollierte Sphäre, in der die Nutzerinnen *allein zu den Bedingungen der Datenverarbeiterinnen* Kontrolle über die sie betreffenden – oder wie bei einem webbasierten E-Mail-Angebot sogar ihnen gehören – Informationen haben. Was daran also eine „gemeinsam“ kontrollierte Sphäre sein soll, erschließt sich nicht.

[1834] Siehe Spiekermann und Cranor (2009, S. 73).

[1835] Siehe dazu und zum folgenden Gürses und del Alamo (2016, S. 42) mit Verweis auf Palen und Dourish (2003) und Nissenbaum (2010).

[1836] Wenig überraschend folgt auf eine Kritik an den ersten beiden Ansätzen *keine* Kritik am dritten...

[1837] Siehe Rost und Pfitzmann (2009) und Bock und Rost (2011). Siehe zur Verankerung der Datenschutz-Schutzziele im Recht Bock und Meissner (2012), die allerdings im engeren Sinne nur die „Vereinbarkeit“ der Datenschutz-Schutzziele mit dem Recht nachweisen. Das ist allerdings wenig überraschend, denn die Datenschutz-Schutzziele wurden schlicht, wie Rost dem Autor in einem Gespräch auf direkte Nachfrage eingestand, aus den gesetzlichen Regelungen abgeleitet. Das heißt aber auch, dass *genau diese* Schutzziele nur vor der Folie des deutschen – und allenfalls des europäischen – Rechts Geltung verlangen können. Es handelt sich damit eigentlich nicht um Datenschutz-Schutzziele, sondern um Datenschutz*rechts*-Schutzziele. Eine Ableitung von Schutzzielen aus der Theorie des Datenschutzes steht damit noch aus. Siehe umfassend zum Problem der Vermittlung von Recht und Technik Rost und Storf (2013).

[1838] Siehe Bock und Rost (2011, S. 32).

[1839] Siehe Rost (2012b). Zu Beginn bezogen sich die Autoren noch auf Ereignisse statt Informationen, siehe Rost und Pfitzmann (2009, S. 356). Prozesse sollen dabei „gesteuert-regulierte[] Abläufe“ sein, die aber – ohne Begründung – zugleich Rollen beinhalten sollen, siehe Rost (2012b, S. 434 f.).

und sehr hoch –, die einfach aus dem BSI-Grundschutz übernommen und für den Datenschutz angepasst wurden, schlägt Rost ein „standardisiertes Datenschutzmodell“ vor, das sowohl für die Gestaltung wie für die Prüfung von Verfahren und ihren Komponenten Soll und Ist kontrolliert aufeinander zu beziehen erlaubt,[1840] und zugleich die Einbindung von Schutzmaßnahmen ermöglicht.[1841] Als „Standard-Datenschutzmodell“ wurde es im Herbst 2015 von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder beschlossen und von Michael Friedewald et al. zur Grundlage eines Vorschlags für eine Datenschutz-Folgenabschätzung nach Art. 35 EU-DSGVO gemacht.[1842]

Während das Standard-Datenschutzmodell auf der Annahme basiert, dass Datenschutz nur durch eine Kombination von rechtlichen, organisatorischen und technischen Maßnahmen sichergestellt werden könne, weil es nicht um den Schutz der Daten, sondern den Schutz der Betroffenen gehe, postuliert Carmela Troncoso in einer Dissertation über Analyse- und Designmethoden für „privacy technologies“ eine – an Spiekermann und Cranors „privacy-by-policy“ und „privacy-by-architecture“ erinnernde – strikte Trennung zwischen „soft“ und „hard privacy guarantees“ und verlangt, dass „privacy-preserving systems“ so zu designen und entwickeln seien, dass sie „hard privacy guarantees“ bieten.[1843] Die Notwendigkeit, rechtliche und organisatorische Maßnahmen als untauglich abzuschreiben, folgt dabei allerdings aus einem Irrtum – oder auch einer Lüge: Die Autorin geht davon aus, dass die Datenverarbeiterinnen „trusted“ seien oder sein müssen – sowie, korrekterweise, kompetent –, damit „soft privacy guarantees“ funktionieren würden,[1844] wobei sie aber übersieht oder verschweigt, dass das Verhältnis zwischen Datenverarbeiterinnen und Betroffenen nicht auf Vertrauen basiert, sondern auf Überprüfbarkeit, die mittels Zuweisung von Begründungs- und Nachweispflichten an die Datenverarbeiterinnen umgesetzt und mittels

[1840] Siehe Rost (2012b). Die Anwendbarkeit des Schutzstufen-Modells auf den Bereich des Datenschutzes wird an keiner Stelle nachgewiesen oder auch nur überzeugend begründet – gleiches gilt für Oetzel und Spiekermann (2012, S. 134) –, und die Ausführungen zu „Religionszugehörigkeit oder medizinische[n] Daten“ lassen die Schutzstufen willkürlich ausgewählt und zugeordnet erscheinen, siehe S. 436. Dafür werden fünf sehr sinnvolle Datenschutz-Risiken aufgeführt: das „Verfahrensrisiko“ als Risiko, das für eine Person durch ein Verfahren erzeugt wird, das „Modellierungsrisiko“ als strukturell defizitäre Datenschutzprüfung, das „Schutzmaßnahmen-Risiko“ für fehlende oder unwirksame Schutzmaßnahmen, das „Kompetenzrisiko“ für unzureichende Ressourcen, fehlende Kenntnisse und Fähigkeiten sowie mangelnde Motivation auf Seiten der Prüferinnen, die sich dann in defizitären Prüfungen widerspiegeln, sowie das „Gesetz- und Kontrollrisiko“ für den Fehlschluss aus der Existenz von Datenschutzgesetzen und Datenschutzbeauftragten auf die Wahrung von Datenschutz, siehe S. 438. Alle fünf Risiken lassen sich auf den Bereich der Technikgestaltung übertragen.

[1841] Siehe etwa Probst (2012), Hansen (2012) und Hansen et al. (2015).

[1842] Siehe Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2015) und Friedewald et al. (2016). Siehe zu letzterem zum Vergleich Wright und Raab (2012) für einen Vorschlag für ein „surveillance impact assessment“ – breit, aber schwammig und teilweise an Beliebigkeit grenzend – und Cavoukian (2010) für die „sieben grundlegenden Prinzipien“ von Privacy by Design – schmal und schwammig, und eben dafür fundiert kritisiert von Seda Gürses, Carmela Troncoso und Claudia Diaz, siehe Gürses et al. (2011). Dabei erzeugt die Formalisierung des Modells jedoch – wie auch jede Prozeduralisierung – das Problem, dass das formalisierte Modell – oder eben der Prozess – an die Stelle einer inhaltlichen – oder materiellen – Prüfung tritt. Es ist nicht mehr notwendig, ein datenschutzfreundliches System – was auch immer das im Einzelfall heißen würde – zu gestalten oder auch nur ein datenschutzrechtskonformes, sondern es müssen nur die Anforderungen aus dem Modell erfüllt werden. Dabei ist klar, dass das Modell keineswegs alle sich aus dem Recht ergebenden Anforderungen in Schutzziele abbildet, siehe etwa Feja et al. (2010, S. 159) zum Problem der Zulässigkeit sowie zu den Betroffenenrechten, aber die Modelldarstellungen explizieren das an keiner Stelle selbst. Und zuletzt hat sich auch die Erkenntnis, dass sowohl die Impact-Assessment- wie die Entwicklungsprozesse verstetigt werden müssen, weil sich sowohl der Einsatzkontext wie auch die Schutzbedarfe mit der Zeit ändern, siehe umfassend Hansen und Thomsen (2010), offensichtlich nicht durchgesetzt.

[1843] Siehe Troncoso (2011).

[1844] Siehe dazu und zum folgenden Troncoso (2011, S. 3 f.).

interner, externer und Betroffenenkontrolle abgesichert wird. Der Vorwurf ist umso absurder, weil ihr Konzept von „hard privacy guarantees“ auf PETs abzielt, die – wie Troncoso selbst feststellt – nicht immer Datenvermeidung, sondern unter Umständen auch nur Datenminimierung garantieren, mit der Folge, dass wie unter den Bedingungen von „soft privacy guarantees“ die Betroffenen, nachdem sie die Daten gegenüber den Datenverarbeiterinnen preisgegeben haben, „little control on how these data are later processed or shared“ haben.

Während es im Bereich des Security Engineering inzwischen zu einer Konsolidierung hinsichtlich der Konzepte, Designprinzipien, Vorgehensweisen und Standards, aber auch der Werkzeuge – oder zumindest bestimmter Klassen von Werkzeugen – gekommen ist, liegt noch ein relativ weiter Weg vor der Entwicklerinnen-Community, die nicht *security*, sondern *privacy*, Datenschutz oder *surveillance* als Anknüpfungspunkte für die Technikgestaltung betrachten. Darüber hinaus kranken die existierenden vergleichenden Arbeiten am gleichen Problem wie die *privacy*-, Datenschutz- und *surveillance*- und die darauf bezogene Systementwicklungsdebatte insgesamt: Sie legen jeweils ihre eigenen, aus beliebigen Quellen oder einfach aus der Luft gegriffenen Verständnisse von dem, worum es gehen soll, an die Vorschläge für Entwicklunsgmethoden an und verhindern damit im Kern sowohl eine Vergleichbarkeit der Methoden wie auch der Vergleichbarkeitsstudien selbst.[1845] Zumindest werden diese Probleme inzwischen grundsätzlich erkannt, wenn etwa auf die unterschiedlichen Verständnisse von und Erwartungen an *Privacy by Design* und die Notwendigkeit zu einer Einigung hingewiesen wird oder auch wenn die Grenzen technischer Systeme und der Technikgestaltung wieder deutlicher hervorgehoben werden.[1846]

Dass Kritik alleine nicht ausreicht, zeigt sich in Versuchen, die bestehenden Ansätze in ein umfassendes Entwicklungsmodell zu integrieren, das Entwicklungsmethoden und Systemansätze vereinigt. In dem von der ENISA herausgegebenen Report „Privacy and Data Protection by Design – from policy to engineering“ werden zwar Prinzipien, die der Technikgestaltung zugrunde gelegt werden sollen, aus dem europäischen Datenschutzrecht abgeleitet – Rechtmäßigkeit, Einwilligung, Zweckbindung, Erforderlichkeit und Datenminimierung, Transparenz, Betroffenenrechte, Informationssicherheit, Verantwortlichkeit und Datenschutz by Design und by Default –,[1847] aber erstens wird dabei nicht transparent gemacht, welche rechtlichen Anforderungen nicht durch diese Prinzipien abgedeckt werden, und zweitens folgt vor allem die Darstellung der technischen Mechanismen einer eigenen, nicht explizierten Logik, bei denen es sich darüber hinaus fast ausschließlich um IT-Sicherheits- und Anonymitätsmechanismen handelt.[1848] Während ENISA zwischen Design-Strategien – „minimise“, „hide“, „separate“ und „aggregate“ als datenorientierte und „inform“, „control“, „enforce“ und „demonstrate“ als prozessoriente Strategien – und Design Pattern unterscheidet, schieben Michael Colesky et al. noch eine Ebene von „tactics“ dazwischen: „approaches to privacy by design which contribute to an overarching strategy“, und Nicolás Notario et al. versuchen, „goal-oriented“ und „risk-based“ Ansätze zu verbinden, indem sie in Reihe geschaltet werden: Erst soll mit einem zielorientierten Ansatz Unsicherheit absorbiert und eine Menge konkreter *privacy*-Anforderungen generiert werden, um anschließend mit einem risikobasierten Ansatz für die systemspezifischen Risiken jeweils konkrete Lösungsansätze zu ermitteln.[1849] Und aus dem oben angesprochenen Whitepaper von Friedewald et al. lässt sich dann auch für die Entwicklung informationstechnischer Systeme die Forderung hinzunehmen, dass zu Beginn einer solchen Systementwicklung die beiden Ziele bestimmt und

[1845] Siehe etwa Beckers (2012, S. 575 f.) und van Rest et al. (2014, S. 59 f.).
[1846] Siehe zu ersterem Kung (2014, S. 181), zu letzterem Klitou (2014, S. 100 ff.).
[1847] Siehe Danezis et al. (2014, S. 7 ff.).
[1848] Siehe dazu Danezis et al. (2014, S. 22 ff.).
[1849] Siehe Danezis et al. (2014, S. 18 ff.), Colesky et al. (2016, S. 1) und Notario et al. (2015, S. 153).

transparent gemacht werden müssen, die verfolgt werden sollen: Erstens ist zu fragen, ob es sich um eine „Marketing"-Entwicklung handeln soll, die „mit geringem Aufwand [...] einen Nachweis über die Erfüllung datenschutzrechtlicher Anforderungen zu erbringen" in der Lage ist, eine „Standard"-Entwicklung („im engeren Sinne") oder gar eine „wissenschaftliche" Entwicklung, „die sich eher in der Tradition wissenschaftlicher Technikfolgenabschätzungen" versteht und das Ziel verfolgt, auch „unbekannte Eigenschaften und Risiken einer Technologie oder eines Systems aufzudecken". Zweitens ist der Fokus zu bestimmen, also ob nur ein technisches System entwickelt werden soll, dass dann in verschiedenen Kontexten eingesetzt werden kann, oder ob für das zu entwickelnde System auch schon der Einsatzkontext feststeht, der dann vollständig im Analyse- und Entwicklungsprozess mit abgebildet werden muss.[1850]

2.6.6 Privacy-Enhancing Technologies

Neben den anonymitätsgarantierenden Kommunikationssystemen, die seit den 1980er Jahren durchgängig diskutiert, erforscht, entwickelt und eingesetzt werden, lassen sich als die drei größten Baustellen im Bereich der Privacy-Enhancing Technologies in den letzten eineinhalb Dekaden die Identitätsmanagementsysteme, die der Idee des „reference monitor" aus den 1970er Jahren folgenden – und trotzdem immer wieder als neu verkauften – Middleware-Ansätze sowie die vor allem im Datenbankenbereich diskutierten formalen Anonymisierungsansätze identifizieren, die auf jeweils relativ unterschiedlichen Bedrohungsmodellen basieren. Hinzu kommen Attribut-basierte Credentials, die unter anderem auf Chaums Idee der „blind signatures" aus den 1980er Jahren basieren[1851] und es erlauben, Eigenschaften nachzuweisen, ohne die Eigenschaften oder die den Eigenschaften zugrunde liegenden Informationen aufdecken zu müssen.

Diese Attribut-basierten Credentials sind – neben dem „obligation manager" genannten „reference monitor" – einer der zentralen Bausteine der Systemarchitektur, die das PRIME-Projekt – und das Nachfolgeprojekt PrimeLife – entwickelt hat.[1852] Das von PRIME zugrunde gelegte Angreifermodell[1853] ist fundamental defizitär: Zwar werden explizit auch Insider, „that [are] involved in the user's transactions", als Angreiferinnen identifiziert, aber aus der Ereigniskette „attack" → „discover information" → „gain some kind of advantage" wird das eigentlich nur als Mittel zum Zweck genutzte „discover information" zum eigentlichen Schutzgut erklärt; Technikgestaltungsziel soll nämlich sein, „[to] prevent the mere possibility to snoop private data." Die Fähigkeit von Insidern, die Transaktion selbst oder die Informationen, die sie im Rahmen der Transaktion erhalten haben, zur Grundlage von Entscheidungen zu machen, um „some kind of advantage" zu erhalten, etwa „to minimize the risk of a policy" im Versicherungsbereich, wird

[1850] Siehe Friedewald et al. (2016, S. 21 f.). Siehe dazu auch schon Rost und Bock (2012, S. 744 f.).

[1851] Siehe Chaum (1983).

[1852] Siehe grundlegend Hansen et al. (2004) und Camenisch et al. (2005). Dass Umsetzungen dieser Projekte in der Praxis nicht zu entdecken sind, liegt sicher auch daran, dass eines der zentralen Probleme zwar klar erkannt wird – „people have little choice but to fill out the mandatory fields of web forms", sie könnten aber auch nicht einfach die Anbieterin wechseln, denn „in practice there is a power imbalance" –, die Lösung dafür aber in Technik liegen solle, die es ermögliche, dass „the user can express a privacy policy which states how her personal data should be handled" und damit „*negotiate* with her transaction partners and conclude an agreement that forms contractual provisions on the privacy rights and obligations of the parties involved in the transaction. Such agreements serve as legal contracts that must be fulfilled by the transaction partners", siehe Camenisch et al. (2005, S. 21), Hervorhebung im Original. Wo plötzlich die Verhandlungsmacht herkommen soll, erklären die Autorinnen leider nicht.

[1853] Siehe dazu und zum folgenden Clauß et al. (2005).

einfach und begründungslos ignoriert.[1854] Stattdessen wird dann einfach in solchen Fällen von den überbordenden Versprechungen der Informatikerinnen[1855] zurückgetreten, und an die Stelle technischer – und als beweisbar *privacy* garantierend markierter – Systeme werden soziale – vor allem rechtliche und institutionelle – und auf die Erzeugung von Vertrauen gerichtete Mechanismen gesetzt.[1856] Und im Laufe des wird der Anwendungsbereich – und damit der Schutzbereich – noch weiter eingeschränkt: „We stress again that in case two PRIME-enabled parties interact, only the part of the interaction that is related to privacy and identity management is governed by PRIME", wobei offensichtlich ein sehr beschränktes Verständnis von *privacy* zugrunde gelegt wird, denn „[t]he architecture is definitely not concerned with business processes such as the data processing by services-side applications. The boundary between PRIME and application is where data leave the PRIME system for processing by applications. It is assumed that business applications only do processing according to the data handling policies."[1857]

Die bereits beschriebenen – auch im PRIME-Projekt eingesetzten – Middleware-Ansätze werden seit der Jahrtausendwende ausgiebig diskutiert, die auf verschiedenen Ebenen – etwa als Teil der Software-Plattform oder als eigenständiges System – und für verschiedene Zwecke – vom simplen Tracking über die Steuerung des Zugriffs auf personenbezogene Informationen bis zur Steuerung der Nutzung bestimmter Systemfunktionen auf Informationen – eingesetzt werden können.[1858] Neben Vorschlägen, die auf einen Einsatz in informationsverarbeitenden Organisationen zielen, gibt es auch einige wenige, die auf Betroffenenseite zur Anwendung kommen sollen.[1859] Alle diese Ansätze setzen auf formale Sprachen für die Beschreibung der Rechte und Pflichten ein, auf deren Basis die „reference monitors" ihre Entscheidungen über Zugriffsgewährung oder -ablehnung sowie weitere Aktionen wie Protokollierung treffen sollen.[1860] Soweit erkennbar, gibt es in diesem Bereich fast keine Diskussion zur Frage, inwieweit diese Policy-Sprachen mächtig genug sind, um alle – etwa aus rechtlicher Sicht – erforderlichen Entscheidungsbedingungen abbilden zu können.[1861]

Obwohl die zwei wesentlichen Bezugspunkte der *privacy*-Debatte im Datenbankbereich bereits in den 1960er und 70er Jahren „erfunden" und diskutiert wurden – k-Anonymität und „statistical disclosure control"[1862] – und k-Anonymität auch schon seit Ende der 1990er wieder

[1854] Siehe dazu auch die Darstellung in Ardagna et al. (2010, S. 124), wo PRIME-Projektbeteiligte dieses Problem zumindest in Teilen adressieren und dabei sogar nicht nur preisgegebene, sondern auch den Betroffenen zugeschriebene Informationen problematisieren, ohne dass daraus allerdings Konsequenzen gezogen würden. Und zumindest Acquisti verdeutlicht sehr gut für einen wichtigen Teilbereich, wie innerhalb von Transaktionen Preisdiskriminierung funktioniert, auch wenn die Transaktion selbst anonym vorgenommen wird, siehe Acquisti (2008, S. 48 f.).

[1855] Siehe Clauß et al. (2005, S. 92).

[1856] Siehe etwa Andersson et al. (2005, vor allem S. 557 f).

[1857] Siehe Sommer et al. (2008, S. 13).

[1858] Siehe beispielhaft aus der sehr breiten Diskussion Karjoth et al. (2004), Gritzalis (2004), Boneh et al. (2004), Berghe und Schunter (2006), Casassa Mont (2006a), Lioudakis et al. (2007) und Ardagna et al. (2010).

[1859] Siehe etwa Pettersson et al. (2006), Hartzog (2009) oder Holtz (2010).

[1860] Siehe oben die Auseinandersetzung mit P3P sowie Backes et al. (2004) für einen Vergleich zwischen den formalen Privacy-Policy-Sprachen.

[1861] Die Ausnahme scheint Holtz und Schallaböck (2011) zu sein, die jedoch ihre Ankündigung, ihre Untersuchungen zu erweitern, offensichtlich nicht umgesetzt haben.

[1862] Siehe etwa Miller (1969, S. 1216 f.), Steinmüller (1970, S. 88) und Dalenius (1977). Bei k-Anonymität und seinen Abkömmlingen werden die Daten nicht verändert, auch nicht bei der Ausgabe – es werden nur keine auf ein Individuum zurückführbaren Informationen ausgegeben. Hingegen werden in den auf „statistical disclosure control" aufsetzenden Ansätzen die Daten durchaus verändert, nur die statistischen Aussagen sollen hinreichend gleich bleiben.

auf dem Tisch lag,[1863] hat die Debatte erst gegen Mitte der nuller Jahre an Fahrt gewonnen. Einerseits wurden die Ansätze zu k-Anonymität sukzessive weiterentwickelt, nachdem sich die jeweils vorhergehenden Vorschläge als unzureichend herausgestellt haben,[1864] andererseits wurde mit „Differential Privacy“ ein – gegenüber Dalenius' ursprünglichen Vorstellungen, die sich als unmöglich erwiesen hatten, weniger weitreichender, aber dafür praktisch umsetzbarer – Vorschlag für eine „statistical disclosure control“ vorgestellt,[1865] für die inzwischen gezeigt werden konnte, dass es zwar keine Äquivalenz, aber eine starke Verbindung zwischen beiden Strömungen gibt.[1866] Die Tatsache, dass in der *privacy*-Debatte im Datenbankbereich die Betreiberin der Datenbank nicht als Angreiferin betrachtet wird und werden kann, wird hingegen – jedenfalls von den Beteiligten an dieser Debatte – nicht problematisiert.

Die derzeit umfassendste Übersicht über den Stand von Wissenschaft und Technik im Bereich der Privacy-Enhancing Technologies bietet der Ende 2015 von der ENISA herausgegebene Report „Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics“,[1867] wenn auch wegen seiner Ausrichtung auf „Big Data“ und deren Nutzung vor allem mit Blick auf traditionelle, zentral organisierte Datenverarbeitung in Organisationen. Vergleichbare Arbeiten für dezentrale Informationssysteme, Kommunikationssysteme, den Bereich der zwischenmenschlichen Datenverarbeitung oder gar solche, die über das enge Verständnis von *information privacy* und Datenschutz im Sinne des derzeitigen Datenschutzrechts hinausgehen, existieren augenscheinlich nicht.[1868]

2.6.7 Die aufkommende Kritik

In den letzten Jahren ist zunehmend Kritik an zentralen Annahmen der *privacy*-, Datenschutz- und *surveillance*-Konzeptionen, Bezugspunkten der Debatten, rechtlichen Regelungsansätzen und der Richtung, die die Technikgestaltung genommen hat, laut geworden. Im Zentrum der Debatte steht dabei das Konzept der informierten Einwilligung.[1869]

Zwar gibt es schon länger Kritik an der Einwilligung, vor allem hinsichtlich ihrer konkreten Ausgestaltung und den daran angeknüpften Folgen,[1870] aber über die Jahre ist nicht nur die Kritik schärfer und mit empirischen Daten unterlegt worden, sie hat auch den politischen Charakter der Fixierung auf die Einwilligung als zentralem Rechtfertigungsgrund für private Datenverarbeitung aufs Korn genommen.[1871] Die empirischen Untersuchungen verweisen auf fundamentale

[1863] Siehe Samarati und Sweeney (1998) und Sweeney (2002b).

[1864] Siehe die Übersicht über die „ursprünglichen“ Ansätze zu k-Anonymität bei Bayardo und Agrawal (2005), die Weiterentwicklungen l-Diversity Machanavajjhala et al. (2007) und t-Closeness Li et al. (2007) sowie die Kritik daran bei Domingo-Ferrer und Torra (2008).

[1865] Siehe Dwork (2006), siehe aber auch die Kritik bei Bambauer et al. (2013).

[1866] Siehe Domingo-Ferrer und Soria-Comas (2015).

[1867] Siehe D'Acquisto et al. (2015).

[1868] Eine Übersicht über die existierenden *privacy*-Metriken, auch wenn ihr Anwendungsbereich ziemlich beschränkt ist oder zumindest sein sollte, bieten Wagner und Eckhoff (2015).

[1869] Arbeiten, die sich nur oder in erster Linie mit spezifischen Besonderheiten des amerikanische *privacy*-Rechts beschäftigen, werden aufgrund des nicht zu erwartenden Erkenntnisgewinns nicht betrachtet.

[1870] In der Bundesrepublik fängt die Diskussion schon direkt nach dem Inkrafttreten des BDSG an, siehe Freiherr von Uckermann (1979). Siehe auch die Darstellung der Debatte bei von Mutius (2004).

[1871] Siehe etwa Hull (2015), der das „privacy self-management“ mit Foucault als „a technology of neoliberal governance“, nicht nur weil es die Verantwortung auf die Betroffenen abwälzt, sondern ihnen zugleich die Schuld für das unausweichliche Scheitern zuschiebt.

Probleme sowohl auf der Informationsseite wie auf der Entscheidungsseite der Einwilligung[1872] und kommen unter anderem zum Ergebnis, dass ein Mehr an Informationen über die möglichen – auch negativen – Folgen der Einwilligung nicht zu mehr Aufmerksamkeit führen, dass aber ein Mehr an *sowohl echter wie vermeintlicher* Kontrolle tendenziell zur Preisgabe von mehr Informationen führt.[1873] Trotz der breiten und fundierten Kritik ist aber eine Lösung nicht in Sicht: Daniel Solove weist zu Recht darauf auf das Problem hin, „[to] limit people's freedom to choose in the name of enhancing their autonomy",[1874] und Benedikt Buchner sieht das Recht auf „Kommerzialisierung der Persönlichkeit" als Ausprägung des – sehr eng verstandenen – Rechts auf informationelle Selbstbestimmung.[1875] Auf der anderen Seite fordert Gabriela Zanfir, den Schwerpunkt auf „suitable safeguards" zu legen, die unabhängig vom Rechtfertigungsgrund für die Datenverarbeitung die Rechte der Betroffenen zu schützen in der Lage seien, und auch Lisa Austin fordert objektivrechtliche Regelungen, die zu einer tatsächlichen Machtbeschränkung der Organisation führen, und knüpft dazu am Rechtsstaatsprinzip an.[1876] Und Paul Ohm schlägt vor, das Prinzip der Einwilligung zwar beizubehalten, aber die Organisation in der Manipulierbarkeit der Einwilligungsbedingungen zu beschränken, indem Unternehmen gezwungen werden, ihren Unternehmens*namen* oder ihr „brand" an selbstdefinierte, aber feste „core privacy commitments" zu binden, bei deren Veränderung der Name des Unternehmens oder des von diesem angebotenen Services geändert werden muss.[1877]

Das zweite Problem, das in den letzten Jahren verstärkte Aufmerksamkeit erfahren hat, ist der konzeptionelle Anknüpfungspunkt der meisten Theorien und der rechtliche Anknüpfungspunkt aller Gesetze im *privacy*-, Datenschutz- und *surveillance*-Bereich: die personenbezogenen Informationen. Das Problem hat drei unterscheidbare Ebenen: Erstens kann es darum gehen zu fragen, ob das Konzept der personenbezogenen Informationen überhaupt ein geeigneter Anknüpfungspunkt für Theorien und Recht sein kann und welche Alternativen es geben kann.[1878] Auf einer etwas konkreteten Ebene stellt sich das Problem, welche Informationen *über Menschen* als personenbezogen gelten sollen und welche nicht.[1879] Und auf der dritten Ebene stellt sich ganz praktisch die Frage, ob konkrete Informationen in einem konkreten Kontext personenbezogen sind oder nicht. Insoweit in den meisten Jurisdiktionen eine Anonymisierung von Informationen eine legale Flucht aus dem Datenschutzrecht ermöglicht, haben die in den letz-

[1872] Dazu gehören etwa die Informationsasymmetrien, das Problem der „bounded rationality", fehlende Selbstkontrolle oder das Zeitproblem – die positiven Folgen der Einwilligung treten sofort auf, die negativen tendenziell später –, siehe grundlegend Acquisti (2004) und Acquisti und Grossklags (2007).

[1873] Siehe dazu Brandimarte et al. (2010), Brandimarte et al. (2013) und Carolan und Castillo-Mayen (2014).

[1874] Siehe Solove (2013, S. 1894). Siehe auch Pohle (2014b, S. 98, Fn. 38) mit dem Hinweis auf das Menschenbild des Grundgesetzes, das – wenig überraschend – genauso idealistisch ist wie die Vorstellungen, die der Einwilligungsfiktion zugrunde liegen.

[1875] Siehe Buchner (2010). Hingegen sieht Iraschko-Luscher (2006, S. 709) eine Notwendigkeit für die Beschränkung der Einwilligung, soweit damit die Gefahr einhergehe, „dass es im Einzelfall zur Aufgabe des bestimmten Hobbys oder Lebensgewohnheit aus rein finanziellen Antrieben kommen könnte", oder wenn etwa „Versicherungen die Möglichkeit an die Hand gegeben würde, politisch mit zu entscheiden, was allgemeinverträglich ist und was nicht". Und Kamp und Rost (2013) wollen eine Einwilligung nur bei echter Wahlfreiheit zulassen, und das sei nicht der Fall, wenn die der Privatautonomie zugrunde gelegte Fiktion des Machtgleichgewichts der beteiligten Privatrechtssubjekte nicht gegeben ist.

[1876] Siehe Zanfir (2014) und Austin (2014).

[1877] Siehe Ohm (2013).

[1878] Historisch lauteten die Alternativen, nur private oder sensitive Informationen als schützenswert zu betrachten oder alle personenbezogenen Informationen. Die umfassendere Konzeption hat sich durchgesetzt, musste sich aber nie als solche rechtfertigen, siehe Pohle (2016b).

[1879] Siehe dazu etwa den Streit um den „relativen Personenbezug" zwischen Article 29 Data Protection Working Party (2007), Weichert (2007) und Pahlen-Brandt (2008).

ten Jahren entdeckten und entwickelten Möglichkeiten zur Re-Identifizierung anonymisierter Informationen „the fundamental inadequacy of the entire privacy protection paradigm based on »de-identifying« the data“ offengelegt.[1880] Schwartz und Solove schlagen deshalb vor, aus einer binären Unterscheidung eine ternäre zu machen, also aus „anonymous“–„identifiable“, wobei letztere sowohl personenbezogene wie personenbeziehbare Informationen umfassen, „anonymous“–„identifiable“–„identified“.[1881] Tatsächlich ist die Beschränkung des Datenschutzes und des Datenschutzrechts auf personenbezogene und personenbeziehbare Informationen selbst defizitär, weil schon lange nicht mehr nur solche Informationen zur Entscheidung über Menschen – und damit zur Beeinflussung der Bedingungen ihrer Freiheitsausübung – genutzt werden, sondern beliebige Informationen. Wenn deshalb Datenschutz und Datenschutzrecht überhaupt beschränkt werden müssen auf den „Schutz der Grundrechte und Grundfreiheiten natürlicher Personen“, wie Art. 1 Abs. 2 der EU-DSGVO statuiert, dann kann einzig sinnvoller Anknüpfungspunkt das Kriterium der „personenbezogenen Entscheidung“ sein.[1882] Und Alessandro Mantelero vollendet, ohne es zu merken, mit seinem Vorschlag, einen Gruppen- oder Kollektivdatenschutz ins Auge zu fassen und die moderne Informationsverarbeitung durch Organisationen, vor allem im Big-Data-Bereich, durch Kollektivakteure oder Institutionen wie Datenschutzaufsichtsbehörden sowie mit Hilfe von Impact Assessments unter Kontrolle zu bringen, den Weg zurück zu den Anfängen der Datenschutzdebatte und dem Konzept des „Datenschutzes im weiteren Sinne“.[1883]

Die anderen Auseinandersetzungen nehmen sich demgegenüber fast ein bisschen bescheiden aus.

So steht die Privat/Öffentlich-Dichotomie inzwischen (wieder) verbreitet in der Kritk, auch wenn daraus oft die falschen Konsequenzen gezogen werden, indem die Forderung nach einer Verstärkung dieser überkommenden Trennung erhoben wird.[1884] Inzwischen finden sich jedoch verstärkt Arbeiten, die diese früh- oder sogar vormodernen Kategorien ablehnen.[1885] Nicht nur wird, wenn die Grundstruktur der sozialen Ordnung auf einen Unterschied von politischer Gesellschaft und häuslicher Wirtschaft reduziert wird, die Realität moderner Gesellschaft als vor-

[1880] Siehe Narayanan und Shmatikov (2010), die sich dabei auf Ohm (2010), der die „legale Flucht“ eine „fair choice“ für Datenverarbeiterinnen nennt, siehe S. 1763, stützen. Seinen Lösungsvorschlag, die bereichsspezifischen Gesetze einfach zu Gesetzen zum Schutz „sensitiver“ Informationen umzudefinieren und dann neue Gesetze dieser Art zu fordern, siehe Ohm (2015), verschweigen wir gerne zum Schutz seines Rufes.

[1881] Siehe Schwartz und Solove (2011). Der Vorschlag geht an der europäischen Rechtsrealität vorbei, weil er die Antwort auf eine nur in den USA stattgefunden habende Entwicklung darstellt, nämlich dass es den amerikanischen Datenverarbeiterinnen gelungen ist, eine Verengung der Definition des PII-Begriffs durchzusetzen, siehe S. 1855 f.

[1882] Siehe Pohle (2016b). In der Konsequenz genauso schon Article 29 Data Protection Working Party (2007, S. 11) auf der Basis einer weiten Definition von personenbezogenen Informationen, wonach „data can be considered to »relate« to an individual because their use is likely to have an impact on a certain person's rights and interests“, ohne dass dieser Ansatz allerdings weiterverfolgt wurde.

[1883] Siehe Mantelero (2016), siehe dazu auch schon Pohle (2016c, vor allem S. 12 f.).

[1884] Siehe dazu schon die Kritik bei Geuss (2001, S. 10) und in der viel später erschienenen deutschen Übersetzung bei Geuss (2013, S. 21): „Die Unterscheidung öffentlich/privat ist eine [...] ideologische Konkretion. Disparate Bestandteile – Begriffsfragmente, Theorien, Volksempfinden, grobe Unterscheidungen, die in sehr speziellen, praktischen Zusammenhängen nützlich sind, stillschweigende Wertannahmen –, die aus unterschiedlichen Quellen stammen und zu verschiedenen Sphären gehören, sind geschichtlich auf unklare Weise zusammengekommen und haben um sich herum so etwas wie ein Kapital der Selbstverständlichkeit, Plausibilität und Motivationskraft angehäuft. Der nicht reflektierte Gebrauch von Unterscheidungen wie dieser hier beschränkt unsere Möglichkeiten, die Welt wahrzunehmen und zu verstehen.“

[1885] Siehe etwa Raigrodski (2013) mit ihrer Kritik an sowohl der Privat/Öffentlich- wie der Haushalt/Markt-Dichotomie.

moderne Gesellschaft beschrieben,[1886] sondern damit werden zugleich das Bedrohungsmodell sowie daraus folgend das Schutzmodell präformiert, an dem sich die Technikgestaltung dann ausrichtet.

Auch das Verhältnis zwischen Recht und Technik sowie zwischen Recht und Technikgestaltung wird inzwischen wieder kritischer beleuchtet, nachdem die sehr naiven Ansätze sowohl in der Rechtswissenschaft wie in der Informatik,[1887] die die Debatte lange dominierten, sich inzwischen als offensichtlich ungeeignet erwiesen haben.[1888] Die Auseinandersetzung ist dabei keineswegs ausgestanden, wie insbesondere die weitverbreitete Fehldeutung des Zweckbindungsprinzips als von der technischen wie gesellschaftlichen Entwicklung überholte *Beschreibung* von vergangenen Praxen organisierter Informationsverarbeitung zeigt.[1889] Klar ist aber jedenfalls, dass eine direkte Übertragung von rechtlichen Regeln in technische Anforderungen nicht funktioniert,[1890] und es noch nicht einmal eine Garantie dafür gibt, dass Regelungen, die auf eine Umsetzung von Datenschutz in Technik zielen, nicht einfach in Regelungen zur Daten*sicherheit* uminterpretiert werden.[1891]

Und nicht zuletzt stehen auch im informatischen Bereich inzwischen weitverbreitete – und doch oft unausgesprochene – Grundannahmen und -paradigmen in der Kritik, angefangen beim fast übermächtigen Fokus auf Geheimhaltung und Vertraulichkeit – und in der Folge davon Verschlüsselung und Anonymität – als zentrale Gestaltungsziele für technische Systeme.[1892]

[1886] Siehe Luhmann (1981, S. 393). In dieser Form zielt die Kritik auf die größten Teile der Soziologie und der Politikwissenschaften, aber auch vieler anderer Geisteswissenschaften. Hingegen bezieht sich die kategoriale Trennung zwischen „öffentlich“ und „privat“ in der bürgerlichen Rechtswissenschaft auf das Gegensatzpaar Staat/Gesellschaft, das genauso überkommen ist, und deshalb zu Recht in der Frühphase der Datenschutzdiskussion abgelehnt wurde, siehe schon Steinmüller et al. (1971, S. 53). Siehe dazu umfassend Pohle (2016a).

[1887] Für den Bereich der Rechtswissenschaft sei hier vor allem auf Lessig und seine Adeptinnen verwiesen, für den Bereich der Informatik sowohl auf die weitverbreitete Unsitte, selbst nach deutlichen Hinweisen auf die Komplexität der Materie und die Rolle, die etwa Kommentare für die Auslegung von Gesetzen spielen, zu glauben, Informatikerinnen könnten „einfach“ die *einschlägigen* Gesetze finden, sie lesen und dann verstehen, *denn die seien ja auf Deutsch geschrieben*, sowie auf die unzähligen Versuche, automatisierte Systeme für die Extraktion von Anforderungen aus Gesetzen zu entwickeln. Siehe zu beidem, wenn auch aufgrund der Beispiele mit einem starken Einschlag des französischen Rechts, Gutwirth et al. (2008), das zugleich indirekt sehr gut erklärt, woran der Datenschutz im Datenschutzrecht „gescheitert“ ist: Er war Rechtspolitik – „regulation“ – und rechtspolitisch gut begründet, ist jedoch dann in die Hände der Juristinnen gefallen und wurde solange durch den Prozess der Reproduktion des Rechts im Recht gedreht, bis er nur noch Datenschutz*recht* war.

[1888] Allein schon, dass es offensichtlich Jahre gebraucht hat, bis den Forscherinnen im Bereich des Requirements Engineering jemand erklärt hat, dass EU-Richtlinien keine hinreichenden Rechtsquellen seien, weil sie grundsätzlich erst in das nationale Recht der Mitgliedstaaten umgesetzt werden müssen, um dann als nationales Recht Geltungskraft zu erlangen, siehe Kiyavitskaya et al. (2008), ist bezeichnend. Und dann stellt sich immer noch die Frage des Umgangs mit prozeduralen Regelungen, die etwa eine Entscheidung auf der Basis einer Abwägung erzwingen.

[1889] Siehe beispielhaft Koops (2011) und zur Klarstellung, dass es sich beim Zweckbindungsprinzip um „die bewusste normative, aber eben auch kontrafaktische Antwort des Rechts auf moderne, grundsätzlich zweckfrei mögliche Informationsverarbeitung“ handelt, siehe Pohle (2015b, S. 143).

[1890] Siehe etwa Koops und Leenes (2013).

[1891] Siehe zu dieser Entwicklung am Beispiel der Datenschutz-by-Design-Regelung im BDSG 1977 Pohle (2015a). Eine der Folgen dieser spezifischen Form von Entwicklungsoffenheit des Rechts – nämlich hin zu einer Absenkung von Anforderungen und Standards – zeigt sich in der relativen Abwehrschwäche gegen die im öffentlichen Diskurs weitverbreitete Ersetzung von Bezugnahmen auf das – gesellschaftlich konsentierte, demokratisch legitimierte und grundrechtlich gebundene – Recht durch Bezugnahmen auf irgendwelche, oft einfach aus den Fingern gesogene ethische oder moralische „Reflexionen“, siehe dazu kritisch Rost (2016).

[1892] Siehe etwa Gürses (2010) und Danezis und Gürses (2010), wobei die Autorinnen als Antwort dann auch wieder nur ihre eigenen unausgesprochenen ideologischen Konstrukte zurückliefern – von der Privat/Öffentlich-

Ähnliches gilt für dezentrale Systeme, die nicht selten in einem überbordend positiven Licht dargestellt werden.[1893]

2.7 Datenschutz zwischen Befindlichkeiten und gesellschaftlichen Machtverhältnissen

Es ist deutlich geworden, dass es weder in der wissenschaftlichen noch in der politischen Debatte eine Einigung zu den unzähligen Aspekten gibt, die im begrifflichen Feld von *privacy*, Datenschutz und *surveillance* liegen. Im Gegenteil: Die Unterschiede zwischen den Beschreibungen, Einordnungen und Erklärungen, die von verschiedenen Seiten geliefert werden, sind so groß und teilweise so grundlegend, dass es geraten scheint, grundsätzlich davon auszugehen, dass in der Debatte schlicht verschiedene Phänomene, Praxen und Probleme von verschiedenen Schulen adressiert werden.[1894]

Schon auf der Ebene des Gegenstandsbereichs gibt es fundamentale Unterschiede, wenn etwa eine Schule ausschließlich interpersonale Beziehungen betrachten will, eine zweite hingegen die Beziehung zwischen Individuen und Organisatione und eine dritte gar die gesellschaftliche Machtverteilung in der Informationsgesellschaft insgesamt. Daraus folgt aber auch, dass die jeweils betrachteten sowie die von der Betrachtung ausgeschlossenen Akteurinnen und deren Verhältnisse zueinander sowie die ihnen zugeschriebenen oder ausgeblendeten Interessen und Eigenschaften, Kenntnisse und Fähigkeiten nicht gleich sind. Nicht überraschend ist es daher, dass es auch keine Einigung darüber gibt, welche Rolle in diesem Bereich informationstechnische Systeme spielen – Automaten, Werkzeuge oder Medien –, von wem sie kontrolliert und wie sie eingesetzt werden, und welche Auswirkungen sie damit jeweils auf die Informationsverarbeitung und Entscheidungsfindung der einzelnen Akteurinnen haben. Weil zugleich die Theorien, die als Raster für die Wahrnehmung der gesellschaftlichen Wirklichkeit dienen, und die disziplinären Hintergründe ihrer Anwenderinnen extrem unterschiedlich sind, ist leider sogar stark zu bezweifeln, dass es auch nur zu einer Einigung auf die Feststellung kommt, welche Unterschiede es denn genau gebe und in welchem Verhältnis die einzelnen Abbilder der Wirklichkeit zueinander stehen.

Vergleichbar groß sind die Unterschiede hinsichtlich der Zielvorstellungen, an denen sich das Informationsgebaren von Individuen, Gruppen und Organisationen, von Privaten und vom Staat oder von der Gesellschaft insgesamt messen lassen muss. Als Schutzgüter werden dabei von den einzelnen Schulen ganz unterschiedliche „Dinge“ identifiziert, von individuellen Zuständen, Bedürfnissen, Interessen oder Werten über soziale Konstruktionen, gesellschaftliche Werte oder Normen bis hin zu Struktureigenschaften von gesellschaftlichen Verhältnissen, aber auch belie-

Dichotomie bis hin zur Fetischisierung interpersonaler Beziehungen. Fundierter ist die Kritik bei Hansen (2012).

[1893] Siehe Narayanan et al. (2012). Siehe auch schon die Kritik bei Agre (2003) an der Vergötterung dezentraler *technischer* Systeme in der Folge der relativ breiten Durchsetzung von P2P-Systemen mit dem Hinweis, die Dezentralisierung technischer Systeme führe nicht automatisch zur Dezentralisierung von Macht- und Entscheidungsstrukturen. Siehe zu dieser Debatte auch George und King (1991), die zeigen, wie flexibel technische Systeme sowohl zentrale wie dezentrale Macht- und Entscheidungsstrukturen unterstützen – es komme also darauf an, mit welchem Ziel sie entwickelt würden, und damit darauf, wer über diese Ziele entscheide.

[1894] Einen ersten wichtigen Schritt in dieser Hinsicht haben Mulligan et al. (2016) unternommen, die für *privacy* nachgewiesen haben, dass es sich um ein „essentially contested concept“ handelt, das dann auch differenziert adressiert werden muss. Zugleich haben sie mit dieser Arbeit einen ersten Vorschlag für ein analytisches Raster zum Vergleich verschiedener *privacy*-Verständnisse und -Theorien vorgelegt.

bige Kombinationen davon. Und so vielfältig wie die Schutzgüter sind auch die verwendeten Bezeichner. Hinzu kommt, dass weder von der Gleichheit noch von der Ungleichheit der Bezeichner darauf geschlossen werden kann, dass gerade die gleichen oder gerade unterschiedliche Schutzgüter adressiert werden.

Und damit überrascht es nicht, dass sich auch die Problembeschreibungen fundamental unterscheiden. Ob Artefakte wie Daten, Informationen oder gar der Computer selbst, Praxen wie Überwachung oder Veröffentlichung, Verdatung oder Missbrauch, Informationsverarbeitung oder -nutzung, besondere Akteurskonstellationen oder deren Eigenschaften wie Machtimbalancen oder Phänomene auf der gesellschaftlichen Ebene wie die Digitalisierung aller Lebensbereiche, die globale Vernetzung oder die Industrialisierung der gesellschaftlichen Informationsverarbeitung – alles ist schon einmal als Problem oder Problemverstärker identifiziert worden. Genauso umstritten sind die Beziehungen zwischen den Akteurinnen, Artefakten und Praxen und die jeweils daraus gezogenen Schlussfolgerungen für die Bestimmung, was Auslöser und was Folge ist, und was davon – Auslöser oder Folge – gerade das Problem bezeichnen soll – von den Einordnungen und Erklärungen ganz zu schweigen. Allein bei der Anknüpfung an personenbezogene Informationen scheint sich eine große Mehrheit einig zu sein – bei gleichzeitiger Uneinigkeit über den Bezeichner – personenbezogene Informationen oder Daten, private oder persönliche Daten, *personally identifiable information*, *personal data* oder *private data* –, das Konzept oder die dahinterstehende Theorie.

Und so unterschiedlich die Problembeschreibungen und -erklärungen sind, so verschieden sind auch die vorgeschlagenen Lösungen. Von sozialen Normen über rechtliche Regelungen oder Marktlösungen bis hin zu technischen Schutz- oder Selbstschutzsystemen wird alles – auch in Kombination – vertreten. Und deren jeweilige konkrete Form wird wesentlich dadurch bestimmt, wer oder was als Problem identifiziert wurde, und welcher Charakter dem Problem zugeschrieben wurde – eine Gefahr, eine Bedrohung oder nur ein Risiko, ausgelöst nur durch Vorsatz oder auch durch Fahrlässigkeit, mit oder ohne Rückgriff auf moralische Wertungen, lösbar oder nur beschränkbar. Und gerade im Zusammenhang mit den Gestaltungsvorschlägen für informationstechnische Systeme ist besonders deutlich geworden, wie sehr es an einem gemeinsamen Ordnungssystem mangelt, denn die Unterscheidung der Technik danach, ob sie Lösung ist oder nur Schlangenöl, kann nur auf der Basis von Angreifer- und Bedrohungsmodell vorgenommen werden.

Offensichtlich ist, wie prekär der allgemeine Stand der Debatte ist. Nicht nur, dass sie sich selbst viel zu wenig reflektiert und die wenigen Einordnungs- und Systematisierungsversuche oft zu oberflächlich sind und in ihrer Abdeckung zu kurz greifen, sie dreht sich auch im Kreis. Immer wieder kehrt sie zurück zu überholten oder längst widerlegten Anknüpfungspunkten, Unterscheidungen und Konzepten. Während die Debatte durchaus stark geprägt ist von Flügelkämpfen und von oft ostentativen Abgrenzungsversuchen, „lebt“ sie gleichzeitig von recht freizügigen Übernahmen – von Rosinenpickerei bis zu ausgemachten Plagiaten. Und die Tatsache, dass wir trotz einer seit 50 Jahren währenden Diskussion über *privacy* und Datenschutz durch Technik – davon zwanzig Jahre unter dem Label „Privacy-Enhancing Technologies“ – von einem breiten Einsatz solcher Systeme weit entfernt sind, ist nicht nur peinlich, sie ist zugleich ein blinder Fleck der Debatte.

In der vorliegenden Analyse ist deutlich geworden, dass viele Konzepte, mit denen in der Debatte operiert wird, aus informatischer Sicht schlicht falsch, nicht, nicht mehr oder nicht vollumfänglich haltbar oder unzulässig verkürzt sind. Dazu gehören etwa die Fixierung auf personenbezogene Informationen sowohl hinsichtlich der Beschränkung des Gegenstandsbereichs als

auch als Anknüpfungspunkt für Rechtssetzung und Technikgestaltung und der daraus folgende Glaube an Anonymität als allgemeingültiger Lösung, die offenkundig falsche und doch weitverbreitete Behauptung, Sensitivität sei eine Eigenschaft von Informationen, die naive Trennung von „öffentlich“ und „privat“, das Konstrukt der informierten Einwilligung, bei der sowohl die Informiertheit wie auch die zur Einwilligung notwendige Freiwilligkeit allzu oft nicht vorhanden ist, oder das sogenannte „Privacy Paradox“.

Darüber hinaus ist festzustellen, dass die Datenschutztheorie zumindest als Theorieschule gescheitert ist. Es ist dieser Schule nie gelungen, eine zugleich umfassende und dennoch lesbare Darstellung ihres Verständnisses vom Menschen und von der Welt, von Organisationen und von der Informationstechnik, von der Informationsverarbeitung und der Informationsgesellschaft vorzulegen, die die eigenen theoretischen Fundamente, Annahmen und Prämissen aufdeckt, das Datenschutzproblem auf dieser Basis fundiert erklärt und die vorgeschlagene Lösung – den Datenschutz – sauber begründet. Als Theorieschule hat sie sich im Grunde nach der Implementation des Datenschutzes im Datenschutzrecht aufgelöst, ihre Mitglieder haben sich vorwiegend dem Datenschutzrecht zugewandt. Sie hat nicht eingegriffen – oder sich sogar daran beteiligt –, als das Problem individualisiert wurde – zurückgestutzt auf die Frage der individuellen Entscheidung über die Preisgabe oder Nichtpreisgabe von personenbezogenen Informationen. Zugleich haben die Diskussion um das Datenschutzrecht, die Gerichtsurteile, vor allem des Bundesverfassungsgerichts, und die Rechtspraxis es geschafft, die theoretische Auseinandersetzung zu dominieren und zu überformen: Die Datenschutzdiskussion ist seit Ende der 1970er Jahre im Grunde nur noch eine Datenschutz*rechts*diskussion, die Mittel stehen im Vordergrund, und um sie dreht sich aller Streit – mit der Folge, dass über Datenschutz nur noch zu den Bedingungen und gemäß den diskursiven Regeln der Rechtswissenschaft diskutiert werden kann. Vor diesem Hintergrund wird es schwer, eine Bindung des Rechts an die Wissenschaft, die das Datenschutzproblem nur erklären kann, und das Politische, wo Datenschutz nur legitim gesellschaftlich ausgehandelt werden kann, zu erzwingen.

Viele Probleme, die die Datenschutzdiskussion bereits in den 1970er Jahren aufgegriffen hat, sind erst in den letzten Jahren wieder breiter diskutiert worden – nur eben nicht mehr als Teil des Datenschutzproblems. Dazu gehören etwa die Probleme gesellschaftlicher Machtverschiebungen, die sich aus den unterschiedlichen Zugangsmöglichkeiten zu und Nutzungsmöglichkeiten von den als „Machtverstärkern“[1895] identifizierten Informatiksystemen für verschiedene gesellschaftliche Akteurinnen ergeben, ob zwischen Staatsverwaltung und Parlament, zwischen dezentralen und zentralen staatlichen oder überstaatlichen Organisationseinheiten, zwischen großen und kleinen Organisationen, für die öffentliche Debatte, für Wahlen und Abstimmungen oder für den Zugang zu Information und Wissen. Die historische Datenschutzdebatte hat früh die Vermessung und Verdatung der Welt problematisiert, die Nutzung von Informationssystemen zur Überwachung von Bevölkerungen, zur Entdeckung von normabweichendem und zur Vorhersage von zukünftigem Verhalten, die Monopolisierungstendenzen von Gatekeepern, die grundsätzliche Beobachtbarkeit jeder technisch vermittelten Kommunikation und die grundsätzliche Zweckfreiheit von Informationssystemen.

Viele ihrer Vorhersagen basierten nicht auf dem damaligen Stand der Technik, sondern auf einer Auseinandersetzung mit den Potentialen, die informationstechnische Systeme besitzen, den Möglichkeiten, die sie ihren Betreiberinnen verschaffen, und einem teilweise naiven Glauben an die damaligen Versprechungen der Herstellerinnen wie auch der Informatik als Wissenschaft, die Systeme mit Eigenschaften für die nahe Zukunft versprach, die sie teilweise erst viele Jahr-

[1895] Steinmüller (1993, S. 417).

zehnte später zu liefern in der Lage waren. Zugleich hat aber diese Mischung aus einer sich an den Potentialen der Technik, den Möglichkeiten ihres Gebrauchs und den Folgen dieses Gebrauchs vor allem durch Organisationen für Menschen, Gruppen, Organisationen und Gesellschaft orientierten Analyse und einer übertriebenen Naivität hinsichtlich der Geschwindigkeit, mit der die Informationstechnik die Gesellschaft durchdringen und ihre „radikale Umgestaltung gesellschaftlicher Verhältnisse“[1896] vollbringen würde, dem Datenschutz – und in der Folge dem Datenschutzrecht – einen deutlichen Vorsprung vor der technischen und gesellschaftlichen Entwicklung verschafft. Und sie hat mit ihrer Bezugnahme auf die Potentiale der Technik – und eben nicht auf den jeweils schnell veraltenden Stand der Technik – dafür gesorgt, dass sie den stärksten Treiber für die technische Entwicklung und den größten Einflussfaktor auf Gestaltung, Auswahl und Einsatz von informationstechnischen Systemen adressieren kann: die Interessen der Datenverarbeiterinnen – und das Datenschutzproblem damit als originär gesellschaftliches.

Vielleicht lässt sich das nirgends deutlicher sehen als beim Umgang mit der Frage nach der Speicherung von Daten „auf Vorrat“, also der Speicherung für unbestimmte Zeit und vor allem für unbestimmte Zwecke: Noch vor wenigen Jahren haben selbst Autorinnen, die sich selbst sehr deutlich als Maßstab der Fortschrittlichkeit angesehen haben, Wirtschaft und Verwaltung jedes Interesse an unbegrenzter Speicherung und Verarbeitung von Daten – im Widerspruch zu ihren eigenen Äußerungen[1897] – abgesprochen und derartige „Befürchtungen“ von Datenschützerinnen als übertrieben abgelehnt,[1898] nur um bald darauf unter Verweis auf genau dieses Interesse – und eine quasi objektive Notwendigkeit in Zeiten von Big Data, Daten unbegrenzt und zweckfrei zu speichern – ein Schleifen des Zweckbindungsgebotes zu fordern.

[1896] Dippoldsmann et al. (1983, S. 420).
[1897] Siehe schon Genscher (1971).
[1898] So etwa Ladeur (2000, S. 18).

3 Die Welt des Datenschutzes

Ausgehend von der im zweiten Kapitel vorgelegten Analyse und Kritik der wissenschaftlichen Auseinandersetzungen um die Beschreibung und Analyse der in der Informationsgesellschaft im Zusammenhang mit moderner Informationsverarbeitung erzeugten individuellen und gesellschaftlichen Probleme, die unter den Labels *privacy*, Datenschutz und *surveillance* diskutiert wurden und werden, sollen nun die Annahmen, der Gegenstandsbereich und die Bedrohungsanalysen einer konkreten Datenschutztheorie und der von dieser Theorie produzierte Datenschutz, mit dem die Bedrohungen abgewehrt werden sollen, kompakt und zusammenhängend re-konstruiert und einer informatisch fundierten Kritik unterzogen werden. Anschließend wird der Datenschutz auf der Basis eines dem Stand der wissenschaftlichen Debatte entsprechenden Angreifermodells und eines daraus abgeleiteten Bedrohungsmodells rekonzeptionalisiert und mit einem neuen Operationalisierungs- und Regelungsansatz versehen. Abschließend soll in aller gebotenen Kürze das für die Technikgestaltung relevante Verhältnis zwischen dem rekonzeptionalisierten Datenschutz und dem geltenden Datenschutzrecht, das historisch wesentlich von der hier betrachteten Datenschutztheorie und ihren Vertreterinnen geprägt wurde und – wenn auch inzwischen weniger – bis heute beeinflusst ist, bestimmt werden, unter anderem im Hinblick auf den Geltungsbereich, den verwendeten Informationsbegriff und das Prozessmodell der Informationsverarbeitung.[1]

Die Analyse und Gestaltung von Informationssystemen, also soziotechnischen Systemen, ist – trotz der weitverbreiteten Selbstbeschränkung der Kerninformatik auf die technischen Teilsysteme solcher Informationssysteme – zentrale Aufgabe der Informatik.[2] Die Betrachtung des gesellschaftlichen Umsystems, in das informationstechnische Systeme eingebettet sind und eingebettet werden, erfordert daher eine Auseinandersetzung mit den Theorien und Methoden, die zur Analyse und zum Verständnis dieses Umsystems, aber natürlich auch des Gesamtsystems, und der Auswirkungen von Informationstechnik, die von der Informatik gestaltet werden, und ihrer Einbettung auf diese Systeme erforderlich sind. Allein kerninformatische Analysen der gesellschaftlichen Probleme, die von und mit informationstechnischen Systemen in ihrer spezifischen gesellschaftlichen Einbettung erzeugt, verstärkt oder verfestigt werden, müssen demgegenüber notwendig verkürzt, verzerrt oder sogar verfehlt sein.

Für die nachfolgenden Ausführungen wird folgende Behauptung als Postulat zugrunde gelegt: Verregelung transformiert die der Verregelung zugrunde gelegten Annahmen in Vorbedingungen, die erfüllt sein müssen, damit durch eine Einhaltung der Regeln das Regelungsziel erreicht werden kann.[3] Daraus folgt, dass der Datenschutz, aber auch das Datenschutzrecht und die dem

[1] Wegen der umfassenden Darstellung im Vorkapitel wird hier weitgehend darauf verzichtet, Wiederholungen mit Quellenangaben auszuzeichnen. Belegt werden aber wörtliche Wiedergaben und im Vorkapitel noch nicht ausgeführte Aspekte.

[2] Siehe Coy (1992) und Coy (2002).

[3] Das Postulat kann hier nur gesetzt, aber aus Platzgründen nicht weiter ausgeführt werden. Es erscheint dennoch sinnvoll, es als Postulat zu explizieren. Für die Technikgestaltung, insbesondere für die Gestaltung von Werkzeugen – im Sinne von Mitteln zu einem Zweck –, als die auch Gesetze gelten können, erscheint das sehr eingängig: Annahmen – etwa über den zukünftigen Verwendungsbereich oder Verwendungszweck –, die der Gestaltung zugrunde gelegt werden, beeinflussen die Gestaltung in mindestens dem Sinne, dass die Technik auf

Datenschutz dienende Technik allenfalls im Rahmen der ihnen zugrunde gelegten Annahmen funktionieren – und damit auch nur in diesem Rahmen Schutz bieten können.[4]

Die Produkte der Datenschutztheorie sind nur Modelle, also vereinfachte Abbildungen dessen, was sie abbilden sollen. Sie basieren auf dem Weltbild – oder den Weltbildern – ihrer Theoretikerinnen. Das erste Produkt ist ein Bild davon, wie diese Theoretikerinnen die Welt sehen, in der sie das Datenschutzproblem verorten, welche Akteurinnen sie in welchen Konstellationen zueinander stehen sehen, welche Eigenschaften – Kenntnisse, Fähigkeiten, Interessen, Mittel – sie ihnen zuschreiben und welche Handlungen sie im Hinblick auf die Erzeugung oder Verstärkung des Datenschutzproblems für zu problematisieren halten. Das zweite Produkt ist das Bedrohungsmodell, das beschreibt und erklärt, welche Bedrohungen für welche Interessen welcher Akteurinnen – der Betroffenen – auf der Basis der Theorie identifiziert werden. Und das dritte Produkt ist ein Bild der spezifischen Erwartungen daran, inwieweit und in welcher Form die Betroffenen vor den identifizierten Bedrohungen geschützt werden sollen, und wie mit und durch Technik – und somit auch durch deren Gestaltung –, vor allem aber durch die Art und Weise des Gebrauchs dieser Technik dieser Schutz gewährleistet werden soll. Die Modelle sind notwendig beschränkt; sie sind nur die Karten zu einem Gelände, die Organigramme zu Organisationen oder die Operationspläne zu Handlungen. Zugleich werden diese Modelle in der vorliegenden Arbeit selbst wieder nur modellhaft, also ohne jeder Verästelung in der Diskussion oder jeder abweichenden Meinung zu folgen, dargestellt.

Die Datenschutztheorie legt die Annahme zugrunde, dass die Gesellschaft, für die sie das Datenschutzproblem analysiert, eine moderne, funktional differenzierte Gesellschaft ist, die von Organisationen geprägt ist und geprägt wird, die rationale Bürokratien im Sinne Max Webers sind, ihre Informationsverarbeitung zum Zwecke – aus ihrer Sicht und in Bezug auf ihre Interessen – besserer Entscheidungsfindung rationalisieren und dazu Computer als Werkzeuge einsetzen. Diese Praxen der Informationsverarbeitung und Entscheidungsfindung durch Organisationen, die dafür eingesetzten Mittel – Technik und Verfahren – und deren Folgen sind es, die sowohl überkommene gesellschaftliche Aushandlungsergebnisse – insbesondere in der konkreten Form, die sie im Recht gefunden haben – wie auch die Aushandlungsmechanismen selbst strukturell unterminieren und deshalb unter Bedingungen gestellt werden müssen. Das Konzept des Datenschutzes stellt sich damit als Ergebnis einer funktionalistischen Analyse dar.[5] Datenschutz ist demnach nicht als Wert an sich – und auch nicht als vor-rechtliches Konzept, das dann in Recht transformiert wird – konstruiert, sondern als ein Mittel in einer bereits verrechtlichten Gesellschaft zur Gewährleistung der Reproduzierbarkeit der Gesellschaft in sich selbst. Datenschutz ist demnach – und darauf hat schon Martin Rost hingewiesen[6] – ein dezidiert bürgerliches Projekt,

diese Annahmen *zugeschnitten* gestaltet wird und anschließend besser für diese Bereiche oder Zwecke geeignet ist als für andere. Dies gilt umso mehr, je stärker das Werkzeug spezialisiert ist – und bei Recht handelt es sich grundsätzlich um ein sehr spezialisiertes Werkzeug, vor allem im privaten Bereich, in dem die bürgerliche Rechtsordnung von den Rechtsgenossen nichts anderes als Rechtstreue fordern kann.

[4] So verweist etwa Priscilla Regan für den US Privacy Act of 1974 auf die Tatsache, dass die konkrete Ausgestaltung der Rechte der Betroffenen im Gesetz auf der Annahme basierte, dass „agencies are using discrete records“, siehe Regan (1988, S. 294).

[5] Das gelte für alle „Problemlösungen“, so Bennett (1991, S. 56) – wenn auch ohne Begründung –, denn „»[t]he »solution« to the problem [...] depends essentially on how the problem is defined.“

[6] Siehe Pohle und Knaut (2014, S. 187, Rn. 204).

jedoch nicht auf der Basis liberal-individualistischer, sondern auf der Basis strukturalistischer Vorstellung davon, wie Gesellschaft „funktioniert“.[7]

Und gerade diese strukturalistisch orientierte Fundierung des Datenschutzes ist es, die den Datenschutz in dem Verständnis, wie er hier dargelegt werden soll, für die Informatik und mithin für die Gestaltung von Informationssystemen und deren technischen Teilsystemen konzeptionell besonders anschlussfähig macht.

3.1 Der Untersuchungsbereich der Datenschutztheorie

Der Untersuchungsbereich der Datenschutztheorie umfasst, so Steinmüller et al. in einem frühen – und zugleich dem konzeptionell saubersten – Versuch einer Absteckung, „die manuelle, die mechanische und die automatisierte“ Informationsverarbeitung in der staatlichen und privaten, „insbesondere unternehmerische[n]“, Verwaltung sowie in der Wissenschaft, denn Datenschutz sei deren „Kehrseite“.[8] Weil Datenschutz „[d]ie Menge der Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung“ sei,[9] folgt daraus, dass das Datenschutzproblem die Menge der unerwünschten Folgen von Informationsverarbeitung bezeichnet. Unerwünschte Folgen seien solche, „die den Zielen unserer Gesellschaft zuwiderlaufe[n] oder sie wenigstens gefährde[n]“, die Ziele hingegen seien „vor allem“ aus dem Grundgesetz zu entnehmen, „namentlich in den Grundentscheidungen dieser Verfassung, die sich bekennt zu einer rechts- und sozialstaatlich verfaßten, das Individuum und die gesellschaftlichen Gruppierungen (insbesondere Minderheiten) schützenden parlamentarischen Demokratie.“

Davon unterscheiden sie – für Juristinnen leider ungewöhnlich, aber konzeptionell sauber – Datenschutzrecht, „[d]ie Menge der Datenschutznormen“. Und im Bereich des Rechts unterscheiden sie dann das „Recht des Individualdatenschutzes“, auch „Datenschutzrecht im engeren Sinne“, das dem „Schutz des einzelnen oder von rechtlich geschützten oder zu schützenden gesellschaftlichen Gruppierungen“ diene, und alle sonstigen Datenschutznormen als „Datenschutzrecht im weiteren Sinne“.[10]

Das „informationelle Selbstbestimmungsrecht“[11] bezeichnet demgegenüber nur das als „Neuinterpretation der Handlungsfreiheit Artikel 2 Absatz 1 GG [erschaffene] Selbstbestimmungsrecht über das individuelle Persönlichkeitsbild“ und stellt nur einen Teil des Fundaments des Individualdatenschutzrechts dar, denn zu diesem gehöre auch die „rechtsstaatliche[] Beschränkung“ der Informationsverarbeitung: „Rechts- und Sozialstaatlichkeit einerseits und Grundrechte andererseits bilden darum die zwei Säulen des DSchRechts.“[12]

In der heutigen Debatte werden hingegen Datenschutz und Datenschutzrecht oft gleichgesetzt. Darüber hinaus beschränkt sich das Datenschutzrecht heute im Prinzip nur noch auf den Schutz individueller Betroffener. Und die Begriffe Individualdatenschutz, Datenschutzrecht im engeren Sinne und Datenschutzrecht im weiteren Sinne sind aus dem Sprachgebrauch verschwunden, auch aus der Fachsprache. Es ist damit im Grunde fast unmöglich, in der derzeitigen Debatte deutlich zu machen, dass das Datenschutzrecht nur eine sehr defizitäre Umsetzung des Daten-

[7] Dies geht noch über den von Bennett angesprochenen Aspekt der Problemdefinition hinaus und adressiert bereits das „Ausgangsmodell“ für die Analyse, das „das Raster [schafft] für die Problemwahrnehmung“ und damit schon Vorentscheidungen über mögliche Problemlösungen trifft, siehe Burkert (1984, S. 184).

[8] Siehe Steinmüller et al. (1971, S. 34 und 45).

[9] Siehe dazu und zum folgenden Steinmüller et al. (1971, S. 44).

[10] Siehe Steinmüller et al. (1971, S. 44).

[11] Der Begriff erscheint in dieser Form auf S. 93, 96, 104, 115, 139 und 140.

[12] Siehe Steinmüller et al. (1971, S. 60).

schutzes ist und dass Datenschutz nicht der ausschließlichen Definitionsmacht der Juristinnen unterliegt, sondern es sich bei Datenschutz um einen ausschließlich aus interdisziplinärer Perspektive begreifbaren Untersuchungsgegenstand handelt.

3.2 Die Umwelt des Datenschutzes

In den frühen Arbeiten zur Datenverarbeitung und zum Datenschutz wird die Gesellschaft durchgängig als moderne, funktional differenzierte Massen-, Industrie- und Informationsgesellschaft verstanden. Schon in den 1960er Jahren sind viele Datenschützerinnen der ersten Generation – so etwa Fiedler, Bull, Simitis und von Berg – an der rechtswissenschaftlichen Debatte um die Verwaltungsautomation beteiligt,[13] andere wie Podlech und – etwas „verspätet“ – Steinmüller arbeiten an der Verbindung von Recht und Informatik.[14] Sie alle waren begeisterte Automatisierungsbefürworterinnen und wurden auch von anderen so wahrgenommen.[15] Sie kämpften dabei gerade auch mit dem Widerstand von Leuten, die ihnen nur ein paar Jahre später den Vorwurf der Automatisierungsfeindlichkeit entgegenschleuderten – die Datenschutzkritikerinnen der 1970er Jahre waren nicht selten die Automationskritikerinnen der 1960er! Die meisten Datenschützerinnen der ersten Generation hatten einen juristischen Hintergrund. Wenig überraschend hat das die Debatte stark geprägt. Überraschender ist, dass nicht wenige der Beteiligten über ein oder mehrere weitere disziplinäre Standbeine verfügten: Herbert Fiedler hat zusätzlich Mathematik und Physik studiert und in Jura und Mathematik promoviert, Wilhelm Steinmüller hat neben Jura auch Theologie, Philosophie und Volkswirtschaft studiert, hat die Rechtsinformatik mitbegründet und wurde später als Professor für angewandte Informatik an die Universität Bremen berufen, und Adalbert Podlech hat vor dem Jurastudium Philosophie, Geschichte und Theologie studiert, sowohl in Philosophie wie in Jura promoviert, bei IBM PL/1 gelernt und später an der Technischen Hochschule Darmstadt versucht, einen Studiengang für Rechts- und Verwaltungsinformatik aufzubauen.

Die theoretische Basis war wenig überraschend stark strukturalistisch geprägt und von Kybernetik und Systemtheorie – sowohl der allgemeinen Systemtheorie Bertalanffys als auch der aufkommenden soziologischen Systemtheorie Luhmanns – beeinflusst. Den größten Einfluss hatte aber sicherlich Max Webers Bürokratietheorie.

Und nicht zuletzt spielte die Erfahrung mit dem Nationalsozialismus eine wesentliche Rolle und die Ende der 1960er und Anfang der 1970er Jahre aus den Diskussionen um die Bayerische Informationszentrale und das „allgemeine arbeitsteilige Informationsbankensystem“ folgende Erkenntnis, in welchem Umfang es der Staatsbürokratie offenbar gelingt, ihre langfristigen

[13] Siehe etwa Fiedler (1964) zum Einsatz von EDV in verschiedenen Verwaltungszweigen, Bull (1964), einer Dissertation über die „Verwaltung durch Maschinen“ und dem Nachweis, dass auch technisches Handeln mit den Kategorien Rechtmäßigkeit und Rechtswidrigkeit bewertet werden könne, Simitis (1967) mit dem Ziel einer optimalen Ausnutzung automatisierter Verfahren in der Verwaltung und von Berg (1968), der in einer Dissertation über „automationsgerechte Rechts- und Verwaltungsvorschriften“ Datenintegration und Zentralisierung als notwendige und erwünschte Folge der Verwaltungsautomation identifiziert (S. 46 ff.). Siehe zur Geschichte der Verwaltungsautomation zwischen Mitte der 1950er und Mitte der 1980er Jahre Brinckmann und Kuhlmann (1990) und knapper, dafür aber über fünfzig Jahre, Lenk (2011).

[14] Siehe etwa Podlech (1969), der die „Rechtskybernetik“ zu einer „juristische[n] Disziplin der Zukunft“ erklärt, Steinmüller (1970), das erste Lehrbuch der in Rechtsinformatik – wegen des schlechten, mit dem „Osten“ assoziierten Rufs der Kybernetik – umbenannten Rechtskybernetik, und Steinmüller (1971b) mit einem Forschungsprogramm für die Rechtsinformatik.

[15] Siehe etwa die Beschreibung von Simitis und seinem Auftreten auf dem 48. Deutschen Juristentag bei Weber (1970).

Datenverarbeitungsprojekte fast unverändert auch über gesellschaftliche Umbruchzeiten hinweg weiterzuverfolgen.[16] Und gerade dabei handelt es sich um eine der Formen der Verselbständigung von Staatsgewalt, die der Rechtsstaat zu verhindern sucht.

In der Debatte wird von den Datenschützerinnen durchgängig der Primat des Rechts gegenüber der Technik vertreten,[17] zugleich aber auch der Primat des Politischen gegenüber dem Recht.

3.2.1 Das Bild der Organisation

Der Analyse des Datenschutzproblems liegt im engeren Sinne keine Organisationstheorie zugrunde, vor allem keine ausgearbeitete. Dennoch lässt sich anhand der in den verschiedenen Texten referenzierten Werke und der verwendeten Begriffe, der Art ihres Gebrauchs und der daraus gezogenen Schlussfolgerungen klar erkennen, dass die Vertreterinnen der Datenschutztheorie die informationsverarbeitenden Organisationen, die sie in den Blick nahmen, als rationale Bürokratien im Weberschen Sinne betrachteten.[18] Explizite Erklärungen dazu, dass gerade Webers Modell zugrunde gelegt wird, sind sehr selten. Christoph Mallmann und – viel später – Alexander Roßnagel stellen die Ausnahme dar.[19]

Weber beschreibt die moderne Staatsverwaltung und große private Organisationen als „bürokratischen Anstalten“. Bürokratie ist dabei die spezifische Form der modernen, rationalen Verwaltung: „Regel, Zweck, Mittel, »sachliche« Unpersönlichkeit beherrschen ihr Gebaren.“[20] Im zweckrationalen Modell Webers ist der Zweck der zentrale Bezugspunkt der Organisationen, der von der Organisation in Bäume von Zwecken und Unterzwecken zerlegt wird, wobei die Unterzwecke jeweils die Mittel zur Erreichung der darüberliegenden Zwecke darstellen.[21] Die Rationalität der Organisation spiegelt sich dann einerseits in der Rationalität der Produktion dieses Zweck/Mittel-Schemas, andererseits in der durch hierarchische Strukturen geprägten und dem Schema angepassten Organisationsgestaltung wider.[22]

Als organisierte Systeme „faktischen Enscheidungsverhaltens“ organisieren sich Organisationen selbst, um Entscheidungsprozesse zu strukturieren, Entscheidungsbedarfe zu regeln und die für die Entscheidungen notwendigen Informationen zu verteilen.[23]

Die Organisationen werden in den einzelnen Arbeiten zum Datenschutz wahlweise als „Organisationen“, „Verwaltungen“ oder „Bürokratien“ bezeichnet, die entweder als „privat“, „öffentlich“ oder „staatlich“ qualifiziert werden, wobei oft aber auch schlicht „Bereich“, „der Staat“,

[16] Siehe unter anderem Hölder (1971) und Genscher (1971) zu den damaligen Vorstellungen der Verantwortlichen sowie Steinmüller (1993, S. 506 f.), Rost und Krasemann (2008), ab Minute 15:40, und Rost und Krasemann (2009) zu den Rückblicken auf diese Diskussionen und deren Einordnungen von Steinmüller und Podlech.

[17] Dabei wird zugleich an eine lange Debatte über das Verhältnis zwischen Gesellschaft, Recht und Technik angeknüpft, die seit mindestens den 1950er Jahren geführt wurde, deren Darstellung aber hier zu weit führen würde.

[18] Siehe Weber (1995, S. 238 ff.). Siehe auch Kühl (2011, S. 23–29) für eine sehr knappe Übersicht über Organisationen aus der Sicht des Weberschen Modells sowie konzeptionell verwandter und ähnlich simplifizierender Modelle.

[19] Siehe Mallmann (1976a, S. 32): „die Datenverarbeitung in der öffentlichen Verwaltung erfolgt zweckrational im Sinne *Max Webers*“, Hervorhebung im Original, und Roßnagel (1989a, S. 133): „Bürokratie wird dabei ganz im Sinne Max Webers als regelgeleitete, aktenbezogene, hocharbeitsteilige, kompetenzgeteilte, hierarchische Organisationsform gesellschaftlicher Herrschaft verstanden.“

[20] Weber (1995, S. 256).

[21] Siehe Kühl (2011, S. 23 ff.).

[22] Siehe Weber (1995, S. 239 f.).

[23] Siehe Luhmann (1966b, S. 14 und 50).

„der Staatsapparat“, „die Wirtschaft“ oder „die Unternehmen“ als Bezeichner genutzt wird. An wenigen Stellen wird die Betrachtung explizit auf „größere“ oder „große“ Organisationen beschränkt.[24] Immer wird ihnen aber zugeschrieben, dass sie rational seien, sich selbst und ihre Informationsverarbeitung rationalisieren würden oder Objekt von Rationalisierung seien, informationstechnische Systeme zur Rationalisierung einsetzen und diese dann rational nutzen würden. Rationalität ist damit neben Automation einer der wesentlichen Bezugspunkte der Datenschutzdebatte in den 1970er Jahren, teilweise auch noch in den 1980er Jahren. Mit der Zeit aber werden beide Begriffe – Rationalität und Automation – in den Texten zum Datenschutz seltener.

Wie schon bei Weber selbst bleibt das Verhältnis zur Organisation notwendig ambivalent: Moderne Gesellschaften sind ohne Organisationen nicht existenzfähig. Menschen sind in modernen Gesellschaften abhängig von Organisationen und ihrer Erbringung von Leistungen,[25] nicht nur, aber auch von zivilisatorischen Grundleistungen. Dabei strukturieren sie „eine Arena für die Betätigung individueller Freiheit“.[26] Organisationen wirken also als gleichzeitig ermöglichende wie beschränkende Struktur.[27]

Die Rationalität der Organisation stellt mit der „Formalisierung bestimmter zentraler Erwartungen“[28] eben auch eine Beschränkung von Willkür dar, und die rationale Vorausplanung ihrer Informationsverarbeitungs- und Entscheidungsverfahren ermöglicht nicht nur deren Formalisierung und Automation, sondern bietet gerade auch einen Ansatzpunkt für die rechtliche Regelung und die Kontrolle von Regeleinhaltung. Besonders deutlich wird dies einerseits in der Konstruktion der Phasenorientierung des Datenschutzrechts, andererseits in der Institutionalisierung der vormals Vorabkontrolle genannten Datenschutz-Folgenabschätzung.

Das Angreifermodell der Datenschutztheorie ist damit schon auf der Akteursebene sehr viel umgrenzter als das der meisten anderen Theorien,[29] auch wenn es weder angemessen anschlussfähig dargestellt noch von allen Beteiligten konsequent zugrunde gelegt und konsistent genutzt wurde. Aus Datenschutzsicht sind damit die Organisationen Angreiferinnen, während Personen grundsätzlich kein Datenschutzproblem erzeugen.[30] Insoweit Datenschutz eine Grenze zwischen dem, was er unter Bedingungen stellen will, und dem, was er nicht betrachten will, zieht, sind

[24] Unter anderem im Gutachten „Grundfragen des Datenschutzes“, siehe Steinmüller et al. (1971, S. 45), „[d]enn nur für größere Informationssysteme besteht ein Regelungsbedürfnis.“

[25] Siehe schon Weber (1995, S. 246 f.).

[26] Luhmann (1964a, S. 384).

[27] Siehe schon in „Grundrechte als Institution“ für den Staat: „Die Grundrechte werden angesetzt, um die Freiheit gegen den Staat zu sichern; aber das setzt voraus, daß zunächst einmal eine Gegeninstanz, ein Monopol auf Freiheitsbedrohung, geschaffen ist, mit deren Bändigung man nicht ins Leere greift, sondern den positiven Erfolg, die Freiheit, wirksam herstellen kann. Der Staat ist, was immer wieder vergessen wird, Vorbedingung aller Freiheit; nicht weil er sie schon partiell oder in elementaren Vorformen gewährleistet, sondern weil sie in der Form des Entscheidungsprogramms für staatliche Organisationen rational regulierbar wird. Der Staat faßt das Potential an Freiheitsbedrohung, das in der Gesellschaft diffus und ungreifbar verstreut vorhanden ist, zusammen und macht die Freiheitsfrage entscheidbar – was im Einzelfall Gewinn oder Verlust der Freiheit bedeuten kann.“ Luhmann (1986, S. 57). In einer modernen, funktional differenzierten Gesellschaft gilt damit auch für alle anderen Organisationen: Wenn sie allgemein oder in einem umgrenzten Bereich ein „Monopol auf Freiheitsbedrohung“ geschaffen hat, existiert ein strukturelles Machtverhältnis, das institutionell eingedämmt werden muss. Siehe dazu auch Luhmanns Verweis auf die Trias der Machtbegrenzungsmechanismen: Grundrechte, Gewaltenteilungsprinzip – oder allgemeiner: Rechtsstaat – und Demokratie – oder allgemeiner: Partizipation –, Luhmann (1986, S. 42).

[28] Luhmann (1964a, S. 384).

[29] Siehe aber Rule (1973) für den Bereich der *privacy*-Debatte sowie Gandy (1989) für die *surveillance*-Debatte.

[30] Es ist wahrscheinlich, dass diese Aussage für die Informatik schwer verständlich ist, daher ein Beispiel zur Erläuterung: Eine einzelne Polizistin, die eine Straftat im Amt begeht, ist kein Rechtsstaatsproblem, sondern ein

Personen, die sich nicht unter Kontrolle der Organisation befinden und die von der Organisation gesetzten Regeln einhalten, als „undichte Dritte“[31] zu betrachten und auszuschließen. Und die Umsetzung dieses Ausschlusses und seine Gewährleistung ist dann Aufgabe der IT-Sicherheit.

Dennoch ist zu fragen, ob und inwieweit das zugrunde gelegte Organisationsmodell tragfähig ist. In der Praxis hat sich schon vor Jahrzehnten deutlich gezeigt, dass die Rationalität der Organisationen sich nicht automatisch in eine Rationalität ihrer Informationsverarbeitungs- und Entscheidungsfindungsprozesse oder die zugrunde liegenden Informationen oder die darauf basierenden Entscheidungen übersetzen.[32] In der Wissenschaft gilt jedenfalls das Webersche Organisationsmodell als überholt,[33] und gerade die Vorstellung in der frühen Datenschutzdebatte ist sehr mechanistisch. Unabhängig von diesen grundlegenden Kritiken stellt sich aber die Frage, ob diese Modellvorstellungen auch für kleine Organisationen gelten. Die meisten Beschreibungen von Organisationen in der Frühzeit der Datenschutzdiskussion beziehen sich auf große Organisationen in Staat wie Wirtschaft, kleine – und damit tendenziell nicht rationale oder nicht rationalisierte – wurden an keiner Stelle explizit problematisiert. Die Frage ist auch, ob „Größe“ ein sinnvolles Maß ist, um die „Rationalität“ und das Bedrohungspotenzial der Organisation und ihrer Informationsverarbeitung zu operationalisieren.[34] Aus informatischer Sicht ist, wie das Beispiel der berühmten Zwei-Personen-„Klitschen“, die in Garagen gegründet werden und „Revolutionen“ auslösen, zeigt, Größe jedenfalls kein sinnvoller Maßstab.

3.2.2 Der Charakter der Informationsverarbeitung

In der Vorstellung der Datenschutztheorie hängen Organisation und Information eng zusammen. Organisationen werden – genauso wie Menschen – als informationsverarbeitende Systeme – auch „Informationssysteme“ – verstanden. Computer sind hingegen datenverarbeitende Systeme, die aber zur Unterstützung der Informationsverarbeitung eingesetzt werden können. Organisationen, die Computer zur Unterstützung ihrer Informationsverarbeitung einsetzen, werden dann als soziotechnische oder techno-soziale Systeme verstanden. Im Gegensatz zu fast allen anderen Theorien in diesem Feld legt die Datenschutztheorie einen ausgearbeiteten und auf Angemessenheit zur Analyse und Lösung des Datenschutzproblems untersuchten Informationsbegriff zugrunde. Vor allem weil der Begriff „Datenschutz“ bereits eingeführt war, als die eigentliche Theoriearbeit gerade erst begann, wurde „Information“ für den juristischen Sprachgebrauch und die Umsetzung im Recht als „Datum“ bezeichnet, was bis heute Verwirrung stiftet. Allerdings ist zuzugeben, dass es in der damaligen Zeit wahrscheinlich auch nicht besser gewesen wäre, am Begriff „Information“ festzuhalten, weil einer der wesentlichen Bezugsrahmen der Debatte – die Informatik – selbst auch einen Informationsbegriff als zentralen Anknüpfungspunkt nutzt, den

individuelles Delinquenzproblem. Wenn die Polizei als Organisation dieses Verhalten deckt, *weil sie Polizistin ist*, dann ist es kein individuelles Delinquenzproblem, sondern ein veritables Rechtsstaatsproblem.

[31] Steinmüller et al. (1978, S. 99).

[32] In den 1980er Jahren fand der Spruch „Wenn Siemens wüsste, was Siemens weiß...“ weite Verbreitung, der das Problem verdeutlicht: Die Organisation als Organisation „weiß“ nicht alles, was die verschiedenen Teile der Organisation „wissen“, und kann es deshalb auch nicht zur Grundlage von Entscheidungen machen. Die zweite Dimension der Aussage bezieht sich auf die Findbarkeit: Die Organisation „weiß“ auch nicht, welche der verschiedenen ihrer Teile was „wissen“, und kann deshalb nicht einmal nachfragen. Ich danke Wolfgang Coy für diesen Hinweis. Siehe dazu auch Luhmann (2000, S. 186) und umfassend Becker (1999).

[33] So jedenfalls Kühl (2011, S. 29).

[34] Die Größe der Organisation findet sich etwa als Maßstab in § 4f Abs. 1 BDSG für die Bestellung von Datenschutzbeauftragten.

Informationsbegriff von Shannon – und der ist gerade wegen seiner Beschränkung auf technische Kommunikationssysteme auch unbrauchbar.[35]

Information dient der Produktion von Entscheidung – für oder gegen eine Handlung – oder Information – als Material für weitere Entscheidungen. Entscheidung ist „erzeugte Information".[36] Entscheiden ist mithin Informationsverarbeitung.

Organisationen entscheiden „in formalisierten systeminternen Verfahrensschritten unter bloßer Orientierung an Programmen und Entscheidungsrastern"[37] – „organisationseigenen Programmen"[38] –, wobei die Informationen aus der Umwelt schon nur über diese „Programme" in die Organisation kommen, *indem* sie intern als Modell erzeugt werden.[39] Solche Modelle sind prinzipiell immer reduktionistisch,[40] aber sie sind dabei nicht falsch, sondern zweckmäßig.[41]

Vor diesem Hintergrund wird verständlich, warum die Datenschützerinnen der ersten Generation eine „modelltheoretische Interpretation des Informationsbegriffs"[42] zugrunde legten. Danach sind Informationen Modelle von Objekten, also Abbildungen. Der Informationsbegriff selbst wurde aus der Semiotik übernommen und besitzt vier Dimensionen: Syntax, Semantik, Pragmatik und Sigmatik. Mit Syntax wird dabei die konkrete, meist zeichenmäßige Repräsentation, mit Semantik die Bedeutung und mithin der Kontext, mit Pragmatik der Zweck und mit Sigmatik der Verweis auf das Objekt – den Menschen, das Ding, das Konzept, das Ereignis oder den Prozess –, das die Information abbildet, bezeichnet.

Diese Abbildungen werden durch die Organisation erzeugt, für ihre eigenen Zwecke und auf ihre Zwecke zugeschnitten. Hier wird der zentrale Unterschied zu Daten deutlich, denn Daten können von Organisationen einfach kopiert werden, Informationen nicht. Die Organisation besitzt damit „Modellierungshoheit":[43] Sie gibt den Zweck vor, mit der die Modelle beschränkt werden, sie entscheidet über die zugrunde zu legenden Modellannahmen und sie kontrolliert die Prozesse der Modellbildung selbst, also die Entscheidungen, welche Ereignisse oder Zustände entweder analysiert oder gerade von der Analyse ausgeschlossen werden, wie sie gemessen und quantifiziert werden, wie sie mit bereits vorhandenen Informationen in Beziehung gesetzt und eingeordnet werden. Information ist damit immer Zuschreibung und kann damit nie objektiv oder neutral sein, aber eben auch nicht sensitiv oder harmlos – sie ist, wie die Organisation sie macht und was sie aus und mit ihr macht und machen will. In der Folge sind die gleichen Daten – unterstellt, dass die Datenformate und Kodierungen gleich sind – für unterschiedliche Organisationen, für unterschiedliche Zwecke, aber auch für unterschiedliche Objekte jeweils grundsätzlich unterschiedliche Informationen.

Zwar werden in der Debatte nicht nur Personenmodelle – „personenbezogene Informationen" im Sprachgebrauch der Rechtsinformatik und „personenbezogene Daten" im Sprachgebrauch des Datenschutzrechts – betrachtet, aber erstens liegt darauf der Schwerpunkt und zweitens werden nur diese – genauer: der Umgang mit ihnen – später im Datenschutzrecht geregelt. Die in den Modellen abgebildeten Personen werden dann in der Sprache des Datenschutzrechts als

[35] Siehe Shannon (1948, S. 379): „ Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem."
[36] Steinmüller (1993, S. 244).
[37] Bischoff (1984, S. 195).
[38] Luhmann (1964a, S. 222).
[39] Siehe zu dieser im System stattfindenden Modellbildung Heylighen und Joslyn (2001).
[40] Siehe Floyd (1985, S. 176).
[41] Siehe Luhmann (1964a, S. 222).
[42] Podlech (1976d, S. 21).
[43] Pohle (2016c, S. 8).

Betroffene bezeichnet. Die Entscheidung für eine Selbstbeschränkung auf Personenmodelle geht dabei – wie in Bezug auf andere Aspekte auch – der eingehenden Analyse des Datenschutzproblems im Laufe der 1970er Jahre voraus.[44] In den nicht so sehr im Zentrum der Aufmerksamkeit stehenden Debatten werden aber auch Gruppenmodelle, Bevölkerungsmodelle und allgemeine Planungsmodelle adressiert und hinsichtlich der Folgen ihrer Verwendung in Organisationen analysiert.

Moderne Organisationen versuchen schon immer, die Grenzen des technisch Machbaren auszuloten und tendenziell alle Informationen zu sammeln, derer sie habhaft werden können, denn wegen des technischen Fortschritts und des damit einhergehenen Preisverfalls ist eine Ausweitung der Informationsspeicherung tendenziell billiger als Löschen, auch weil sich Organisationen damit Entscheidungsmöglichkeiten – und darauf aufbauend organisatorische Entwicklungsmöglichkeiten – offenhalten wollen. So überrascht es auch nicht, dass Einmalerhebung, unbeschränkte Verbreitung innerhalb der Verwaltung und Mehrfach- und Vielfachnutzung personenbezogener Informationen erklärte Ziele der Verwaltungsautomation waren.[45] Die Datenschutzdiskussion hat das durchaus wahrgenommen und als Problem markiert, obwohl das von den Automationsbefürworterinnen propagierte Ziel in deutlichem Widerspruch zur Annahme steht, es handele sich um zweckrationale Organisation.

Die Automation setzt auf der in rationalen Organisation schon stattfindenden Rationalisierung – Formalisierung und Standardisierung der Verfahren, Typisierung der Modelle, Transformation subjektiver in objektive Prozesse – auf. Vergleichbar zur Industrialisierung der physischen Arbeit wird versucht, die Informationsverarbeitung der Organisationen zu „maschinisieren“, also in „maschinen“-verarbeitbare Prozesse zu transformieren.[46] Dazu werden sowohl die Informationen – als Daten – wie auch die Entscheidungsprogramme – auf der Prozessebene als Algorithmen oder Heuristiken, aus der Systemsicht als Software – in informationstechnische Systeme übertragen.[47] Diese können dann zur Unterstützung menschlicher Entscheidungsfindung dienen oder die Entscheidungen selbst treffen. Dabei werden die Typisierungen danach ausgewählt, dass sie sich möglichst gut technisch umsetzen und nutzen lassen. Kriterien aus der Technik bedingen also die Gestaltung der Modelle.

Auch wenn in den verschiedenen Arbeiten nicht immer deutlich gemacht wird, für wie mächtig die Maschine tatsächlich gehalten wird, scheint doch zumindest die Annahme verbreitet zu sein, dass der Computer sich in Richtung eines Informationsverarbeitungssystems – und nicht nur eines Datenverarbeitungssystems – entwickeln werde. Zumindest aber ist allgemeine Ansicht, dass der Computer die Beschränkungen der menschlichen Datenverarbeitungsfähigkeiten aufhebt. Damit einher geht dann aber eben ein qualitativer Sprung in der Informationsverarbeitungs- und Entscheidungskapazität von Organisationen, die diese Maschinen einsetzen. Dieser Sprung wird an vielen Stellen als „radikal“ bezeichnet oder – von Fiedler – als „Übergang zu einer neuen Stufe der Rationalität.“[48]

[44] Von unterschiedlichen Autorinnen werden sowohl Ruprecht Kamlahs 1969 veröffentlichte Dissertation über die amerikanische *privacy*-Debatte als auch der im Spätsommer 1970 in der NJW erschienene Artikel von Ulrich Seidel als Entscheidungspunkte genannt, und zumindest Seidel expliziert, dass „wie im amerikanischen Recht jedes personenbezogene Datum als schutzfähig anzusehen“ sein solle, siehe Seidel (1970, S. 1583).

[45] Siehe Genscher (1971) und Brinckmann et al. (1974, S. 6 ff.).

[46] Steinmüller beschreibt deshalb diese Transformation der gesellschaftlichen Informationsverarbeitung als Industrialisierungsprozess. Eine umfassende Auseinandersetzung mit dieser Einordnung muss an anderer Stelle stattfinden, schon weil die Anschlussfähigkeit dieser Konzeptionalisierung sowohl für die rechtswissenschaftliche wie auch für die informatische Diskussion unklar ist. Für einen Versuch siehe Pohle (2016c).

[47] Siehe zuletzt mit sauberer Unterscheidung Schinzel (2017).

[48] Fiedler (1975, S. 80).

Im Gegensatz zum Organisationsmodell überzeugt der Informationsbegriff bis heute, auch weil er hervorragende Anschlussmöglichkeiten für alle – oder zumindest die meisten – an der Debatte beteiligten Disziplinen bietet, insbesondere für die Soziologie, die Rechtswissenschaft und natürlich die Informatik. Sowohl Verarbeiterinnenwechsel, Zweck- und Kontextveränderungen wie auch Ketten von Interpretationen, Verdatungen und Re- oder Neu-Interpretationen lassen sich damit konsistent unter Bezugnahme auf einen gemeinsamen Informationsbegriff adressieren. Gleiches gilt für die Erkenntnis, dass das Maschinenmodell der Informatik, der Automat, und damit eine Bezugnahme nur auf informationstechnische Systeme für die Analyse der individuellen und gesellschaftlichen Risiken moderner Informationsverarbeitung zu kurz greift.

Problematisch ist hingegen die in der Datenschutzdebatte weit verbreitete – und sehr wahrscheinlich direkt aus der Vorstellung von Zweckrationalität abgeleitete – Unterstellung, Organisationen würden versuchen, ihre Umwelt möglichst auf der Basis von explizierten Modellannahmen zu beobachten, ausschließlich oder vorwiegend kausalitätsbasierte Abbildungen vorzunehmen und deshalb einem objektiven Zwang zur Datenqualität zu unterliegen, an den sich dann das Datenschutzrecht einfach ankoppeln kann, um aus „Fehl"-Interpretationen von Informationen folgende Erwartungsverletzungen auf Seiten der abgebildeten Personen zu verhindern. Aus der Sicht der Organisation ist das aber egal, solange es ihr gelingt, die daraus sich ergebenden Risiken für sich selbst im Rahmen zu halten oder sie auf ihre Klientel abzuwälzen.[49]

3.2.3 Das Technikbild

Der Analyse des Datenschutzproblems liegt fast durchgängig ein instrumentelles Verständnis von Datenverarbeitungstechnik zugrunde, jedenfalls in Bezug auf die Organisation. Informationstechnische Systeme werden als Werkzeug verstanden, die von ihren Beherrscherinnen – ob Herstellerinnen, Eigentümerinnen oder Betreiberinnen – nach ihren Interessen gestaltet und eingesetzt werden. Den Betrachtungen ihrer Folgen – oder besser: den Folgen ihres Gebrauchs – für die Betroffenen liegt aber eher ein relationales Verständnis zugrunde.[50]

Die Technik werde nicht nur nach den Interessen der Datenverarbeiterinnen gestaltet, in der Technik verkörperten sich dann auch diese Interessen und in ihrem Einsatz diene sie ihnen. Das sei auch nicht überraschend, denn die Gestalterinnen und Betreiberinnen seien selbst von einem instrumentellen Rationalismus geprägt.[51]

Aus Sicht der Datenschutzdebatte ist Technik in großem Maße gestaltbar. Bei „technischen Zwängen" handele es sich in den meisten Fällen schlicht um Rechtfertigungsformeln für Eigenschaften, die – ob bewusst oder unbewusst – in informationstechnische Systemen im Interesse ihrer Beherrscherinnen hineinkonstruiert wurden. Sie dienen dazu, sowohl die Tatsache dieses Hineinkonstruierens selbst wie auch die hineinkonstruierten Interessen nicht diskutieren zu müssen. Die Gründe für dieses Nicht-diskutieren-Wollen können vielfältig sein – es kann etwa schlicht sein, dass eine Explikation der Interessen zur Aufkündigung eines vorher mühsam erkämpften Konsenses, der vielleicht auch nur in einer „Unterstellung der Gleichsinnigkeit"[52] bestand, zu führen droht. Für die Datenschützerinnen zählen in erster Linie die Folgen für die Betroffenen,

[49] Siehe zu ersterem Pohle (2014b, S. 95, Rn. 22), zu letzterem Rost (2014b, S. 73).
[50] Siehe zu diesen Technikverständnissen Hildebrandt und Tielemans (2013, S. 511 ff.).
[51] So der direkte Vorwurf von Gandy (1993, S. 80).
[52] Luhmann (2000, S. 92 ff.).

denn die Informationstechnik wird als Machtverstärker verstanden,[53] und daher sei relevant, welche Interessen in der Technik verkörpert werden. Und natürlich, wie die Systeme eingesetzt werden.

Wenn aber die Technik gestaltbar sei und von den Organisationen gestaltet werde, und die Organisationen und ihr Handeln dem Recht unterworfen seien, dann müsste Recht grundsätzlich auch in der Lage sein, so die Argumentation der Datenschützerinnen, die Gestaltung und den Gebrauch informationstechnischer Systeme zu steuern. Beides war daher immer auch explizites Ziel der Datenschutzdebatte. Und insoweit Organisationen zum Zwecke der Optimierung und Rationalisierung von Tätigkeiten diese automatisierten – und vor dem Hintergrund der Diskussion um automationsgerechte Gesetze in den 1960er Jahren –, konnte durchaus erwartet werden – und Fiedler hat sogar explizit gefordert, dass die Gesetze dazu automationsgerecht gestaltet werden sollen –, dass Organisationen Datenschutz in Technik umsetzen – und genau darauf zielte dann auch eine Regelung im Bundesdatenschutzgesetz 1977.[54] Zwei Oberziele wurden dabei formuliert: Technik müsse machen, was sie solle, und Technik dürfe nicht können, was sie nicht dürfe. Oder etwas überspitzter: Wenn die Organisation schon eine (Webersche) Maschine sei, dann könne der (informationstechnischen) Maschine ganz sicher beigebracht werden, sich wie eine sich rechtmäßig verhaltende Organisation zu verhalten.

So zwingend sich diese Argumentation auch anhören mag, so voraussetzungsvoll ist sie doch gleichzeitig – und nur in einem geringen Umfang wurde das in den ersten beiden Jahrzehnten reflektiert.[55] Sehr früh war zumindest schon klar, dass Informationssysteme grundsätzlich zweckfrei seien, und ihre „Multifunktionalität“ wurde breit diskutiert. Und genau deshalb wurde die Einführung des zugleich kontrafaktischen wie normativen Prinzips der Zweckbindung gefordert,[56] wenn es auch erst im BDSG 1990 umgesetzt wurde. Dieses Zweckfreiheitsproblem wurde später differenzierter betrachtet: Computer und Netze seien grundsätzlich zweckfrei, aber mit Programmen – und nur mit diesen – könne der Computer zweckbeschränkt werden.[57] Gleichzeitig sind aber diese Systeme durchgängig nur als sehr geschlossene, ja fast schon totale Systeme imaginiert worden. Das zeigen etwa die umfassenderen Gestaltungsvorschläge, die im Laufe der Debatte vorgelegt wurden, so etwa Podlechs Vorschlag zur Trennung von politischer, technischer und fachlicher Verantwortung direkt im System, wobei die Benutzerinnen (fachliche Verantwortung) nur über definierte Schnittstellen auf die Systeme (der Unternehmerinnen, technische Verantwortung) mit den Daten zugreifen dürfen, auf denen dann die mittels Programmkontrolle kontrollierbare Datenverarbeitung abläuft, Steinmüller et al. mit einem System, das alle Aufgaben einer Institution abbildet und nur genau deshalb kontrollierbar gemacht werden kann, Bräutigam et al. mit dem Vorschlag für eine von keinem Programm umgehbare Middleware oder Hammer et al. mit einem extrem abgeschlossenen System, das gestaltet werden soll, nämlich einem betrieblichen Telefonsystem.[58] In allen diesen Fällen tritt die Technik damit deutlich als reines Instrument der Organisation auf.

Diese Vorstellung mag bis in die 1980er Jahre für den Computer und seinen Einsatz in Organisationen vor allem aufgrund seines Preises, der daraus resultierenden relativ geringen Ver-

[53] Sie wirke zwischen Kapital und Arbeit als Effizienz- oder Rationalisierungstechnik, zwischen Apparat und Klientel als Modernisierungs- oder Verdatungstechnik und zwischen Herrschenden und Beherrschten als Herrschafts- und Kontrolltechnik, so Steinmüller (1993, S. 417).

[54] Siehe Pohle (2015a).

[55] Eine frühe Ausnahme stellt Fiedler (1975) dar.

[56] Siehe Pohle (2015b).

[57] So etwa Steinmüller (1981, S. 154).

[58] Siehe Podlech (1976b), Steinmüller et al. (1978), Bräutigam et al. (1990) und Hammer et al. (1992).

breitung und der Anforderungen an seine Programmierung und Bedienung noch einen gewissen Wirklichkeitsbezug gehabt haben. Aber jedenfalls mit dem Aufkommen des PCs, der breiten Verfügbarkeit von Software – vor allem solcher Programme wie *VisiCalc*, *Microsoft Multiplan* und *Lotus 1–2–3* –, mit dem Erscheinen der ersten einfach nutzbaren grafischen Benutzeroberflächen und mit der zunehmenden Vernetzung der Endgeräte – sogenannten „offenen Netzen", im Gegensatz zur seit den 1960ern schon problematisierten Vernetzung („Integration") von Informationssystemen – verlor der Computer seinen instrumentellen Charakter auch in der Praxis. Und damit wird eben gerade fraglich, inwieweit Organisationen tatsächlich in der Lage sind, ihre automationsunterstützten Informationsverarbeitungsverfahren zu kontrollieren, oder ob es sich dabei – analog etwa zu den Fiktionen im Bereich der informierten Einwilligung (Wahlfreiheitsfiktion, Marktfiktion, Transparenz- bzw. Bestimmtheitsfiktion, Aufsichtsfiktion)[59] – nicht schlicht um eine Kontrollierbarkeitsfiktion handelt.

Die Datenschützerinnen der ersten Generation haben diese Diskussion dann schon nicht mehr geführt, auch wenn sie den Bedarf dafür wahrgenommen haben.[60]

3.2.4 Schlussfolgerungen

Vor diesem Hintergrund zeigt gerade die Verbindung zwischen dem unterstellten zweckrationalen Charakter von Organisation und dem ebenso unterstellten instrumentellen Charakter von informationstechnischen Systemen, dass die heute gerne bemühte Behauptung, das Datenschutzrecht basiere auf der Vorstellung des klassischen Großrechners der 1970er Jahre, fehl geht und zu kurz greift. Richtig ist hingegen, dass sich Datenschutz nach der Vorstellung der damaligen Debatte offensichtlich nur in von kontrollierbaren und sich selbst kontrollierenden Organisationen kontrollierten Informatiksystemen direkt umsetzen lässt. Diese Kontrollierbarkeitsfiktion prägt aber auch stark die informatische Debatte um die datenschutzfreundliche oder *privacy-enhancing* Technikgestaltung, so etwa im Bereich der nutzerinnenkontrollierten Identitätsmanagementsysteme oder bei Apps auf Endnutzerinnengeräten. Gestaltungsziel ist in diesen Fällen offensichtlich immer die – eventuell sogar beweisbare – Garantie von bestimmten Eigenschaften der technischen Systeme. Diese Zielvorstellung, die in Anlehnung an Troncoso[61] als „harter Datenschutz" bezeichnet werden kann, lässt sich damit aber eben offensichtlich nur in einem Teil von Systemen umsetzen, die dann aber datenschutzgarantierend sind.

Wenn die Annahme, dass Organisationen zweckrational sind, Technik unter ihrer vollen Kontrolle steht und die Verfahren nur in oder mit dieser Technik stattfinden, fallen gelassen wird, dann lassen sich allenfalls schwächere Formen des Datenschutzes in Technik und durch Technik umsetzen. Das Ziel ist dann, Technik zu gestalten, die den Datenschutz – als Eigenschaft einer Praxis der Informationsverarbeitung und Entscheidungsfindung – fördert und seine Einhaltung sehr viel wahrscheinlicher macht als seine Nichteinhaltung.

3.3 Das Problem des Datenschutzes

In der frühen Datenschutzdiskussion gab es nicht *eine* konsentierte Problembeschreibung, sondern eher eine Sammlung von als konzeptionell verbunden verstandenen Problemfeldern, die von unterschiedlichen Beteiligten als mehr oder weniger eng zusammenhängend verstanden wurden.

[59] Siehe Kamp und Rost (2013, S. 81 f.).
[60] Oder dies zumindest später behaupten, wie etwa Steinmüller im Interview, siehe Rost und Krasemann (2009), ab Minute 43:20.
[61] Siehe Troncoso (2011).

Das zeigt sich etwa schon an der Trennung zwischen Datenschutz im engeren Sinne und Datenschutz im weiteren Sinne. Einer der Hauptgründe dafür liegt wohl darin, dass diese Diskussion vorwiegend von Juristinnen geführt wurde, von denen viele nicht sauber zwischen Problembeschreibung, Problemlösung und der Umsetzung dieser Lösung im Recht unterschieden, und deshalb die jeweils als Prämisse spezifisch gesetzte Regelungsintention die Problembeschreibung selbst notwendig beschränkte – vergleichbar zum Grundproblem aller Privatheitsdebatten, die sich geradezu sklavisch an den Begriff „privat“ gebunden haben und binden, und insoweit nur Probleme sehen können, die sich als „privat“ markieren lassen.

Als die Datenschutzdebatte begann, war der „Organisationsvorsprung“, also der spezifische Machtvorsprung der Organisationen als Organisationen – begründet in der strukturell besseren Fähigkeit, Informationen zu verarbeiten und Entscheidungen zu treffen –, gesellschaftlich, vor allem durch das Recht, bereits eingehegt. Immer deutlicher wurde jedoch, dass die überkommenen Einhegungsmechanismen, also die Mechanismen, wie sie im Recht konkretisiert und umgesetzt worden waren, unter den Bedingungen der automationsgestützten Informationsverarbeitung nicht mehr funktionierten. Die Datenschutzdebatte versucht, auf dieses Problem eine Antwort zu finden und stellt dabei relativ schnell fest, dass es nicht ausreichen würde, ein paar Änderungen an einzelnen bestehenden Regelungen vorzunehmen. Stattdessen musste das Verhältnis zwischen Organisation, Information, Informationsverarbeitung und Macht grundlegend neu analysiert und auf die Folgen untersucht werden, die entstehen, wenn die Freiheits- und Partizipationsversprechen sowie die Strukturschutzprinzipien und -mechanismen der modernen bürgerlichen Gesellschaft auf Organisationen treffen, die im Zuge und mit Hilfe moderner Informationsverarbeitung diese Versprechen, Prinzipien und Mechanismen strukturell unterminieren.

Vor diesem Hintergrund soll nachfolgend das in der damaligen Debatte oft nur aspektbezogen diskutierte Datenschutzproblem, das sich als Folge der Rationalisierung, Maschinisierung und Automation der Informationsverarbeitung und Entscheidungsfindung in Organisationen ergibt, strukturiert re-konstruiert werden. In einem ersten Schritt werden dazu die dadurch erzeugten oder verbesserten und tendenziell auf Dauer gestellten Potentiale moderner Organisationen zur Steuerung oder Beeinflussung individueller, kollektiver oder institutioneller Betroffener und ihrer Handlungen sowie der Prästrukturierung ihrer Handlungsmöglichkeiten dargestellt. Anschließend werden solche Folgen betrachtet, die sich aus der konkreten Art und Weise der Informationsverarbeitung und Entscheidungsfindung in Organisationen ergeben. Dabei handelt es sich etwa um die Folgen, die sich daraus ergeben, dass Organisationen der Informationsverarbeitung Modellannahmen zugrunde legen (müssen), über die sie selbst die Modellierungshoheit haben, die Informationsverarbeitung grundsätzlich nur gemäß ihrer eigenen Programme und der dieser zugrunde liegenden Funktions- und Verfahrenslogik durchführen können und sie dabei tendenziell zur Aufhebung getrennter Kontexte mit deren jeweiligen Eigenlogiken und spezifischen Rollen und Rollenerwartungen neigen.

3.3.1 Das Problem der Datenmacht

Die durch Rationalisierung, Maschinisierung und Automation verbesserten Informationsverarbeitungs- und Entscheidungsfähigkeiten von Organisationen führen zu einer gegenüber dem schon vorhandenen, sich etwa bereits aus der Arbeitsteilung ergebenden, Organisationsvorsprung nochmals deutlich gesteigerten Leistungsfähigkeit der Organisationen, ihre jeweilige Umwelt wahrzunehmen und in dieser Umwelt – aus ihrer Sicht und in ihrem Interesse – angemessen zu agieren. Es verbessert sich die Fähigkeit der Organisation, Sachverhalte, vergangene und gegenwärtige Ereignisse, die daran beteiligten Akteurinnen und deren Beziehungen zu den Ereignissen

und zueinander sowie deren Auswirkungen zugleich umfassender und in höherer Detailschärfe, schneller und effizienter zu erfassen, intern als Modelle – Informationen – abzubilden und als Daten zu speichern, zu verbreiten, mit anderen Informationen in Zusammenhang zu setzen und zu vergleichen, zu bewerten und darauf basierend Entscheidungen darüber zu treffen, wie sie damit umgeht oder darauf reagiert. Darüber hinaus steigt ihre Fähigkeit, das zukünftige Verhalten der modellierten Objekte vorherzusagen – genauer: sie können die Treffsicherheit ihrer Vorhersagen steigern –, und damit steigen die Erfolgsaussichten, dieses Verhalten zu beeinflussen, zu beschränken oder gar zu verhindern. Die Verdateten – Personen, Gruppen, ganze Bevölkerungen, aber auch andere Organisationen oder Institutionen – werden also, während sie durchleuchtet, verdatet, wahlweise entindividualisiert oder versippenhaftet, jedenfalls aber objektiviert und nummeriert werden, tendenziell unvergessen in Bezug auf die Vergangenheit, vorhersagbar in Bezug auf die Zukunft und mithin kontrollierbar in der Gegenwart. Für eine Einschränkung der Handlungsfreiheit reicht es, wenn die Verdateten damit rechnen müssen – oder auch nur nicht ausschließen können –, dass ihnen diese Handlungen später in solchen vermachteten Verhältnissen zum Vorwurf gemacht werden oder anderweitig Nachteile bescheren. Die konkreten Folgen sind jeweils davon abhängig, in welchem Verhältnis die Organisationen zu den von ihren Entscheidungen Betroffenen stehen.[62] Zu den damals diskutierten Beispielen gehören die Möglichkeit, zum Ziel staatlicher, vor allem polizeilicher Maßnahmen zu werden, neue oder gerichtsfeste Ablehnungsgründe, die sich für eine öffentliche Verwaltung gegenüber Antragstellerinnen eröffnen, Preisdiskriminierungsmöglichkeiten für Unternehmen gegenüber ihren Kundinnen, Entscheidungsmöglichkeiten für Arbeitsgeberinnen über die Begründung oder Beendigung von Arbeitsverhältnissen, für Finanzinstitute über die Kreditkonditionen sowie für Versicherungen über die Versicherungskonditionen. Andere in der Debatte problematisierte Bereiche betreffen Marktbeeinflussung und Monopolisierungstendenzen im Wirtschaftsbereich, das Verhältnis zwischen Arbeitsgeberinnen und Belegschaften in Mitbestimmungsfragen, zwischen Politik und Öffentlichkeit, zwischen Legislative und Exekutive oder zwischen zentralen und dezentralen Organisationseinheiten des Staates.

Einige Eigenschaften dieser Folgenbetrachtung verdienen besondere Aufmerksamkeit: Erstens lädt die abstrakte Beschreibung des Problems dazu ein, es als nur abstrakt existierendes Problem zu ignorieren oder ihm die praktische Relevanz abzusprechen. Zweitens lädt sie dazu ein, es auf der gleichen abstrakten Ebene lösen zu wollen. Das ist etwa beim Code of Fair Information Practices oder bei den OECD Guideline geschehen, die deshalb statuieren, dass die Informationsverarbeitung „fair“ zu erfolgen habe. Drittens transformiert auch die am häufigsten umgesetzte Antwort des Rechts auf eine solche Klasse von Problemen, die Prozeduralisierung, das Problem nur: Wer entscheidet dann nach welchen Maßstäben, und wie sind der Entscheidungsprozess, die konkrete Abwägung und das Ergebnis für wen überprüfbar? Die Maßstäbe sind dann gerade das vierte Problem, denn die Bewertung der Folgen in jedem Einzelfall ist hochgradig interessen- und wertgebunden. Und selbst eine Systematisierung nach „Verwendungszusammenhängen“[63] kann fünftens nicht verhindern, dass die spezifische Systematik – vor allem im privaten Bereich – immer hochgradig umstritten bleiben wird, und darüber hinaus, wie jetzt im öffentlichen Be-

[62] Sie entstehen unabhängig davon, wie sie bewertet werden – als erwünscht, neutral oder unerwünscht –, aber nur auf der Basis der Feststellung der Tatsache, dass sie entstehen, können sie zum Gegenstand einer gesellschaftlichen Debatte gemacht und politisch entschieden werden, um dann – je nach Ergebnis – im Recht Niederschlag zu finden.

[63] Simitis (1973, S. 154).

reich bereits zu beobachten, zu einer Flut von im Verhältnis zueinander immer inkonsistenter werdenden Regelungen führt.[64]

3.3.2 Das Problem der Rationalitätsverschiebung

Der zweite Aspekt, der in der historischen Datenschutzdebatte breit diskutiert wurde, betrifft die Rationalitätsverschiebung und deren Folgen. Organisationen bilden die Objekte aus der Umwelt auf der Basis von Modellannahmen, die unter Modellierungshoheit der Organisationen gemäß den organisationseigenen Zwecken produziert werden, intern ab, unterwerfen sie dann der organisationseigenen Funktions- und Verfahrenslogik und verarbeiten sie entsprechend ihrer eigenen Programme. Sie entscheiden dabei zugleich selbst, welche Objekte sie abbilden und welche nicht. Die Folgen fehlender, falscher, veralteter oder für die intendierten Entscheidungen anderweitig unpassender Informationen tragen jedoch in erster Linie die Betroffenen. Gleiches gilt für die damals wie heute weitverbreitete Unterstellung, dass Informationen in Akten und informationstechnischen Systemen sowohl objektiv wie auch korrekt seien, weil sie in Akten stehen oder in Computern gespeichert sind. Das liegt auch daran, dass Organisationen zum Ignorieren, Verschweigen oder Verstecken ihrer Modellierungshoheit tendieren. Deutlich wird dies etwa bei Statistiken, aber auch Simulationen: Eine Organisation entscheidet, welche Rohdaten auf der Basis welcher Fragestellungen und mit welchen Methoden erhoben werden – und welche nicht –, wie sie gefiltert, verarbeitet, verknüpft und analysiert werden – und dann wird damit „Politik“ gemacht, etwa mit der Polizeilichen Kriminalstatistik oder Bevölkerungsprognosen, oder „Wissenschaft“ wie bei Google Trends. Mehr noch: Weil die Zwecke die Modellannahmen (mit-)produzieren, kann Korrektheit grundsätzlich allenfalls für den Zweck sichergestellt werden, der den Modellannahmen zugrunde gelegt wurde. Auch über Sachverhalte treffen Organisationen Vorentscheidungen in einer Weise, die dazu führten, dass nur noch entschieden werden kann, was die Organisationen an Entscheidungsspielraum noch übrig gelassen haben. Ob es sich dabei um Kundinnen gegenüber Unternehmen, Rezipientinnen gegenüber Inhaltsanbieterinnen, Gerichte gegenüber Geheimdiensten, politische Gremien gegenüber der öffentlichen Verwaltung oder die Wahlbevölkerung gegenüber dem Staat handelt, führt strukturell zum gleichen Ergebnis: Ohne Aufdeckung der Vorentscheidungen und der zugrunde liegenden Entscheidungsprämissen lässt sich für die Betroffenen nicht effektiv prüfen, welche Entscheidungsalternativen weggefallen sind und ob die verbleibenden nicht zufällig alle die Eigenschaft haben, den Interessen der Organisationen zu dienen. Im Ergebnis okkupieren damit die Organisationen die ursprünglich den Betroffenen gehörenden Entscheidungsräume – ein Problem, das in den 1970ern vor allem am Beispiel der Machtverschiebung zwischen Parlament und Ministerialbürokratie in Gesetzgebungsverfahren diskutiert wurde. Hinzu kommt, dass die in diesen Informationsverarbeitungsprozessen erzeugten „Datenschatten“[65] nicht an das Objekt gebunden sind, das sie „hervorgebracht“ hat. Ihrer beliebigen Speicherung, Verwendung und Weitergabe steht damit nichts mehr im Weg. Sie verstetigen damit nicht nur alte – und möglicherweise überholte – Sachverhalte, sondern sie ersetzen zugleich das Objekt, das sie repräsentieren, und ermöglichen es damit der Organisation, Entscheidungen über die verdateten Betroffene zu treffen, ohne mit der Betroffenen interagieren zu müssen.

[64] Und genau das muss Simitis 25 Jahre später dann auch eingestehen: „Eine zunehmend am einzelnen Verarbeitungskontext orientierte Interpretation verengt den Blick auf partikuläre Aspekte und verkürzt zusehends die Reichweite der Leitprinzipien des Datenschutzes“, siehe Simitis (1998, S. 2475).

[65] Westin (1967, S. 163 ff.) und Anér (1972, S. 179).

Dieses von der Organisation erzeugte Problem findet seine Entsprechung im Bereich der informationstechnischen Systeme. Während die Debatte in den Anfangsjahren vor allem auf die Substitution menschlicher Informations- durch technische Datenverarbeitung in den Organisationen zielte und dabei etwa problematisierte, dass Code an die Stelle von Recht trete, aber nicht öffentlich und damit auch nicht überprüfbar sei, sind später auch Endnutzerinnensysteme in den Blick genommen worden, etwa als mit ISDN plötzlich für Angerufene sichtbar wurde, wer anruft – Verwaltungen konnten nun vor dem Abheben schon zwischen erwünschten und unerwünschten Anruferinnen, etwa Journalistinnen und anderen Querulantinnen, unterscheiden. Inzwischen haben sich die Bereiche, in denen Probleme mit versteckten Modellannahmen und der Entscheidungsraumokkupation auftreten können, bedeutend ausgeweitet – von Googles Entscheidung, aus Berechenbarkeitsgründen Relevanz aus Empfängerinnensicht durch Relevanz aus Senderinnensicht zu ersetzen, bis zu Facebooks Kontrolle über die Auswahl der Quellen für den Newsfeed und die Trending Topics.

3.3.3 Das Problem der Entdifferenzierung

Die zunehmende Integration von Informationssystemen führt, so lässt sich der dritte große Diskussionsgegenstand der Datenschutzdebatte zusammenfassen, zur tendenziellen Aufhebung der die moderne, funktional differenzierte Gesellschaft prägenden Trennung zwischen gesellschaftlichen Subsystemen, Feldern oder Kontexten mit jeweils spezifischen Eigenlogiken. Die Versuche der Organisationen, die differenzierten Rollen, in denen Menschen in modernen Gesellschaften mit Organisationen interagieren, zusammenzuführen, um „das »Eigentliche« der Person“[66] aufzudecken und zur Grundlage der eigenen Informationsverarbeitung und Entscheidungsfindung zu machen, gefährdet dabei nicht nur die Menschen, die sich in der Folge mit rollenfremden Erwartungen konfrontiert sehen. Sie gefährdet auch die moderne Gesellschaft und die Existenz der gesellschaftlichen Autonomiebereiche schlechthin, denn diese basieren gerade auf der Aufrechterhaltung ihrer jeweiligen Eigenlogiken gegenüber den Eigenlogiken anderer Bereiche – „sachwidrige Koppelung“[67] ist ein Gesellschaftsstruktur-Problem, nicht nur ein individuelles. Als besonders schweres, nämlich als Problem des Schutzes der Menschenwürde wird das Problem der Aufhebung der Rollentrennung gefasst, wo es in individualisierter Form als Problem der Erstellung umfassender Persönlichkeitsbilder adressiert wird, denn den Menschen in seiner ganzen Persönlichkeit zu erfassen, degradiere ihn zum Objekt.[68] Aus Sicht der Datenverarbeiterin jedenfalls bestimmt sich, so viel dürfte heute klar sein, die Umfassendheit eines Profils nach dem Zweck, den die Datenverarbeiterin verfolgt, und das liegt mindestens dann vor, wenn „es

[66] Müller (1974, S. 82).
[67] Schlink (1973, S. 159).
[68] In der Praxis allerdings bietet selbst das absolute Verbot der Erstellung umfassender Persönlichkeitsbilder, siehe BVerfGE 27, 1, 6, keinen Schutz, denn es ist nur ein Schreckgespenst: In der Entscheidung zur Online-Durchsuchung hätte das BVerfG wegen der realen Möglichkeit, ein umfassendes Persönlichkeitsbild erstellen zu können, und der gleichzeitigen Unmöglichkeit, diese Erstellung zu verhindern, die Online-Durchsuchung für grundsätzlich verfassungswidrig erklären müssen. Das hat es aber gerade nicht. Erst beschwört das Gericht die Gefahr des umfassenden Persönlichkeitsbildes, die mit jedem Totalzugriff auf den Computer notwendig einhergeht. Als „Lösung“ statuiert es mit dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein neues Grundrecht, das jedoch zentral auf den Kernbereich privater Lebensgestaltung adressiert. Damit wird ein vormals als wirksame Grenze für staatliches Informationshandeln angesehenes Schutzobjekt erst auf einen Teilaspekt reduziert (Kernbereichsschutz) und damit einer Abwägung zugeführt, die mit prozeduralen Schutzmaßnahmen die staatliche Maßnahme ermöglicht, siehe BVerfG (2008, S. 311 und 335 ff.).

das künftige Verhalten der Person prognostizierbar macht oder den Rollenwechsel des einzelnen [...] unmöglich macht."[69]

3.3.4 Schlussfolgerungen

Der Kern des Datenschutzproblems sind also die strukturellen Machtimbalancen, die durch die Rationalisierung, Maschinisierung und Automation gesellschaftlicher Informationsverarbeitungsprozesse erzeugt, verstärkt oder verfestigt werden, und deren Folgen für Individuen, Gruppen, Organisationen und die Gesellschaft insgesamt.

Der gesellschaftliche Bedarf nach Datenschutz als „Lösung" des Datenschutzproblems entsteht demnach, wenn die Freiheits- und Partizipationsversprechen sowie die Strukturschutzprinzipien und -mechanismen der modernen bürgerlichen Gesellschaft auf Organisationen treffen, die im Zuge und mit der Industrialisierung der gesellschaftlichen Informationsverarbeitung diese Versprechen strukturell unterminieren. Datenschutz ist demnach die informationelle Dimension der „Lösung" des allgemeinen gesellschaftlichen Machtproblems.

Die einzelnen Problembereiche wurden für verschiedene Konstellationen unterschiedlich umfassend und tiefgehend analysiert. Schon damals bildeten Analysen, die Personen als Betroffene in den Blick nehmen, mit großem Abstand die Mehrheit der Ausarbeitungen, und inzwischen wird fast nichts anderes mehr betrachtet. Das Problem des Gruppendatenschutzes, im 1971er Gutachten noch ein wichtiger Teil des Individualdatenschutzes, blieb lange eher unterbelichtet oder wurde in Nebensätzen abgehandelt, die sich im Kern mit Personendatenschutz beschäftigten. Inzwischen scheint dem Gruppendatenschutz jedenfalls wieder ein wenig mehr Aufmerksamkeit zuteil zu werden.[70] Wenn überhaupt eine Diskussion zu Organisationen oder Institutionen als Betroffenen von Datenmacht stattfand oder stattfindet, dann fast nie im Rahmen der Datenschutzdebatte, jedenfalls nicht nach den 1970er Jahren. Das Gleiche gilt für die Gesellschaft als Ganzes.

Ein Grund für diese Schlagseite der Debatte findet sich darin, dass gerade die Arbeiten, die die ganze Breite der Betroffenen in den Blick genommen haben, den Fokus der Analyse auf die Datenverarbeiterinnen legen und versuchen zu ermitteln, wie sich aus welchen Gründen welche Machtverschiebungen zugunsten dieser Organisationen ergeben. Es handelt sich hier in gewisser Weise um das ebenso problematische Gegenstück zu einem Großteil der *privacy*- und Privatheitsdebatte: Indem in Akteurskonstellationen ein zu starker Fokus auf eine Seite dieser Konstellationen gelegt wird – in der Datenschutzdebatte auf Organisationen als Datenverarbeiterinnen, in der *privacy*-Debatte auf Personen als Betroffene –, bleibt die andere Seite fast notwendig unterbelichtet. Im organisationsfixierten Teil der Datenschutzdebatte sind die Betroffenen oft dann einfach nur „Alle", während in der personenfixierten *privacy*-Debatte dieses „Alle" auf die Angreiferinnen verweist.

Ein zweites – und fast noch größeres – Problem liegt im inzwischen ausnahmslosen Fokus auf ein spezielles Mittel, das in den Angriffen der Organisationen auf die Betroffenen verwendet wird: den personenbezogenen Informationen. Diese, jeder Analyse schon vorausgehende, Fixierung auf personenbezogene Informationen stellt eine mehr als fragwürdige Selbstbeschränkung hinsichtlich des Untersuchungsgegenstandes dar und produziert dabei fast schon absurde Konsequenzen: Es wird als *privacy*-, *surveillance*- und Datenschutzproblem für Alice und ihre Freiheitsausübung wahrgenommen, wenn diese Freiheitsausübung im Zuge oder infolge der Verarbeitung personenbezogener Informationen über Alice beschränkt wird, nicht aber, wenn das im

[69] Siehe Steinmüller et al. (1971, S. 97).
[70] Siehe etwa jüngst Mantelero (2016).

Zuge oder infolge der Verarbeitung personenbezogener Informationen über Bob geschieht. Diese Selbstbeschränkung, die in der wissenschaftlichen Debatte schon konsentiert war, bevor die Datenschutzdiskussion Ende der 1960er Jahre begann,[71] ist zwar an einigen Stellen „umgangen" worden, etwa wenn die Machtverschiebungen mit einem ausschließlichen Fokus auf die Organisationen, die diese Machtverschiebung verursachen, beschrieben wurden, aber in der Mehrzahl der Arbeiten wurde sie einfach unreflektiert übernommen, wenn nicht sogar gepriesen.[72]

Im Grunde ist für die Grenzziehung zwischen Informationen, deren Umgang problematisiert werden soll, und solchen, die aus dem zu betrachteten Gegenstandsbereich ausgeschlossen werden, nur für die innere Grenze, also die Einbeziehung von bestimmten Informationen, eine Begründung – ob wissenschaftlich oder politisch – gegeben worden. Die Außengrenze jedoch wurde nie begründet, sondern nur statuiert. Die hingegen wahrlich oft zu findende Aussage, die ausgeschlossenen Informationen würden gerade ausgeschlossen, weil sie nicht personenbezogen seien, ist gerade keine Begründung dafür, dass nur personenbezogene Informationen betrachtet werden, sondern schlicht das Ergebnis der notwendig scheiternden Subsumtion dieser Informationen unter den Personenbezugsbegriff.

3.4 Die Architektur des Datenschutzes

Auf der Basis der vorherigen Ausführungen lässt sich damit der historisch konstruierte Datenschutz als Lösung des Datenschutzproblems systematisch nachzeichnen. Dazu gehören sein Gegenstandsbereich und seine Ziele sowie seine funktionale Regelungsarchitektur.

3.4.1 Der Gegenstandsbereich des Datenschutzes

Der Gegenstandsbereich des Datenschutzes umfasst alle sozialen Beziehungen, die von einer strukturellen Machtimbalance geprägt sind, in der die mächtigeren Akteurinnen als Folge ihrer qualitativ besseren Informationsverarbeitungs- und Entscheidungsfähigkeiten in der Lage sind, Verhaltensmöglichkeiten für die schwächeren Akteurinnen zu beschränken, deren Verhalten zu beeinflussen oder gar zu steuern, die gesellschaftlich ausgehandelten Freiheitsräume zu schließen und die Aushandlungsprozesse zu manipulieren sowie die Funktionsbedingungen der bürgerlichen Gesellschaft zu unterminieren.

Die Beziehung zwischen Individuen und Gruppen auf der einen und privaten und öffentlichen Organisationen auf der anderen Seite stellt dabei den klassischen Fall einer solchen Beziehung dar, unabhängig davon, ob die Personen oder Gruppen als Bürgerinnen dem Staat gegenübertreten, als Kundinnen den Unternehmen, als Kreditnehmerinnen oder -geberinnen den Banken, als Rezipientinnen den Medien, als Patientinnen den Gesundheitsinstitutionen, als Arbeitnehmerinnen den Arbeitgeberinnen oder als Mitglieder den Vereinigungen. Dazu gehören entsprechend auch Beziehungen zwischen Vereinigungen der strukturell Schwächeren und denen der Mächtigeren wie etwa im Bereich betrieblicher Mitbestimmung, im Bildungs- und Ausbildungsbereich oder zwischen Oppositions- und Regierungsfraktionen. Auch gesellschaftliche Institutionen wie „die Öffentlichkeit" sind in ihrem Verhältnis zu strukturell übergriffigen Akteurinnen wie dem Staat, vor allem Geheimdiensten und Militär, der Wirtschaft, den Medien oder anderen

[71] Siehe Pohle (2016b, S. 15 f.).

[72] Das entspricht in etwa einer Fixierung auf blaue Messer: Sie sind scharf und spitz und können genutzt werden, um Menschen zu verletzen. Deshalb müssen sie reguliert werden. Grüne Messer sind auch scharf und spitz und können auch zum Verletzen von Menschen benutzt werden, aber sie sind eben nicht blau und müssten daher nicht reguliert werden.

Gatekeepern Teil dessen, was der Datenschutz adressiert. Darüber hinaus problematisiert der Datenschutz das Verhältnis zwischen kleinen und großen Organisationen, vor allem wenn letztere Oligopolisierungs- oder Monopolisierungstendenzen zeitigen. Auch das Verhältnis zwischen Parlamenten und der Rechtssprechung auf der einen und der Exekutive auf der anderen Seite, zwischen unter- und übergeordneten Organisationseinheiten des Staates, aber auch zwischen Organisationen, deren Aufgabe darin besteht, die Machtbeschränkung anderer Organisationen zu kontrollieren und abzusichern, und den von ihnen kontrollierten Organisationen können in den Bereich des Datenschutzes fallen.

Kurz: Datenschutz beobachtet die informationellen Beziehungen zwischen Schwachen und Starken, zwischen Kleinen und Großen, zwischen Minderheiten und Mehrheiten, zwischen Unten und Oben, zwischen Lokalen und Globalen, zwischen Exkludierten und Inkludierten und bezieht Position für die Schwächeren.

Vor diesem Hintergrund wird deutlich, warum die doppelte Beschränkung des Datenschutzes – einmal auf Individuen als Betroffene und dann zweitens auf den Bereich des Umgangs mit sie betreffenden personenbezogenen Informationen –, wie sie heute fast ausschließlich diskutiert wird, vollkommen am Datenmachtproblem vorbeigeht – fast wie eine auf Dienstage beschränkte Rechtsstaatsgewährung. Jedenfalls die erste Beschränkung ist im Wesentlichen ein Artefakt des bürgerlichen Grundrechtsverständnisses, das gesellschaftliche Probleme grundsätzlich nur durch die Brille des Individuums und damit individualisiert sehen kann, um sie erst auf dieser Basis wieder zu vergesellschaften.[73] Nur selten gelingt im Einzelfall eine Überwindung dieser Beschränkung; so etwa bei der Aufnahme des mit dem Datenschutz strukturell vergleichbaren Umweltschutzes in das Grundgesetz.[74]

3.4.2 Das Ziel des Datenschutzes

Datenschutz heißt, informationell begründete soziale Macht in der Informationsgesellschaft unter Bedingungen zu stellen, sie zu zwingen, sich zu verantworten, und sie damit (wieder) gesellschaftlich verhandelbar zu machen. Seine Funktion besteht darin, dass kontingente Sozialstrukturen sich auch unter den Bedingungen der Industrialisierung der gesellschaftlichen Informationsverarbeitung und gegen die „überlegen standardisierende Strukturierungsmacht von Organisationen“[75] reproduzieren können.

Datenschutz zielt dabei auf alle drei einander ergänzenden „Klassen“ von Machtverhältnisse konditionierenden Verfassungsinstitutionen:[76] erstens die objektivrechtlichen und auf gesellschaftlich akzeptable Strukturreproduktion gerichteten Organisationsprinzipien, vor allem das Rechtsstaatsprinzip, zweitens die Grundrechte als individuelle Abwehr- und zugleich Teilhaberechte und drittens das zum Partizipationsprinzip verallgemeinerte Demokratieprinzip. Da-

[73] Und genau in einem solchen Zweischritt, der einen „Umweg“ über das Individuum darstellt, verweist das BVerfG im Volkszählungsurteil auf die objektiv-rechtliche Funktion des Rechts auf informationelle Selbstbestimmung: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“ (BVerfG, 1983, S. 43).

[74] „Der Staat schützt auch in Verantwortung für die künftigen Generationen die natürlichen Lebensgrundlagen und die Tiere im Rahmen der verfassungsmäßigen Ordnung durch die Gesetzgebung und nach Maßgabe von Gesetz und Recht durch die vollziehende Gewalt und die Rechtsprechung.“ – Artikel 20a GG.

[75] Zimmermann (2014, S. 58, Rn. 35).

[76] Siehe Luhmann (1986, S. 42).

tenschutz schützt also *die* Ordnung, die Freiheitsräume und Freiheit produziert und Teilhabe garantiert. Datenschutz schützt die individuelle und kollektive Wahrnehmung von Freiheit und Teilhabe sowie deren Bedingungen und Umstände. Und Datenschutz schützt die gesellschaftlich legitimierten Aushandlungsprozesse, die diese gesellschaftliche Ordnung produzieren, reproduzieren und verändern.

Datenschutz beobachtet Informationsverarbeitungs- und Entscheidungsverfahren in Organisationen sowie Kommunikationsbeziehungen in vermachteten sozialen Beziehungen, beurteilt deren Fairness, ermächtigt die informationell Schwächeren und beschränkt die informationell Stärkeren.

Datenschutz ist damit die Bedingung der Möglichkeit von Freiheit und Teilhabe in einer durch Organisationen und ihre Informationsverarbeitung strukturierten Gesellschaft.

Zugleich dient der Datenschutz – und das ist kein Widerspruch, sondern weist den Datenschutz gerade als bürgerliches Projekt aus – der Produktion von gesellschaftlicher Akzeptanz von organisierter Informationsverarbeitung und deren Industrialisierung, der Schaffung von Systemvertrauen und mithin der Gewährleistung der Akzeptabilität der Informationsgesellschaft.

3.4.3 Der abstrakte Einhegungsmechanismus des Datenschutzes

Der Datenschutz bedient sich der relativ erfolgreichen Präzedenzen von gesellschaftlichen – vor allem rechtlichen – Einhegungen von strukturellen gesellschaftlichen Machtimbalancen in der bürgerlichen Gesellschaft, vor allem im Bereich von staatlicher und politischer Macht.

Aus den bereits genannten, gesellschaftliche Machtverhältnisse konditionierenden Verfassungsinstitutionen in Verbindung mit dem zweckrationalen Organisationsmodell, das der Datenschutztheorie zugrunde gelegt wurde, lassen sich sechs Anknüpfungspunkte für Mechanismen zur Einhegung von Datenmacht ableiten: Zwecke, Organisationsstrukturen, Mittel, Kontrolle, Transparenz und Intervenierbarkeit. Aus der historischen Datenschutzdebatte lassen sich jedoch nur für den Bereich des Individualdatenschutzes diese Anknüpfungspunkte nachzeichnen. Für die anderen Bereiche des Datenschutzes sind – jedenfalls im Rahmen der als Datenschutzdiskussion markierten Debatte – allenfalls allgemeine oder unspezifische Forderungen in dieser Richtung erhoben worden, etwa die Forderung nach der Einführung eines Parlamentsinformationssystems, das dem Parlament einen eigenen, von der Regierung nicht kontrollierbaren Zugriff auf das damals geplante Regierungsinformationssystem erlauben sollte. Im Folgenden wird daher nur der Bereich des Individualdatenschutzes betrachtet.

Im Individualdatenschutz – nachfolgend einfach Datenschutz – wird der Schutz vor der Datenmacht der Organisation umgesetzt durch Einflussnahme auf die Zwecke der Informationsverarbeitung, auf die Struktur der Organisation und auf die Mittel – Informationen, Prozesse und informationstechnische Systeme –, die die Organisation einsetzt, durch die Institutionalisierung von Kontrollstrukturen, durch Transparenzpflichten für die Organisation sowie durch Interventionsmöglichkeiten für die Betroffenen.

„Zweck“ ist der zentrale Begriff im zweckrationalen Organisationsmodell und das Leitprinzip, nach dem Organisationen ihre eigenen Strukturen gestalten, die Mittel auswählen und ihre Praxen ausrichten. Der Datenschutz nutzt den – von der Organisation selbst gewählten oder ihr von außen vorgegebenen – Zweck als konstant gesetzten Prüfanker und zwingt die Organisationen, sich selbst, die Gestaltung und Wahl ihrer Mittel sowie deren Einsatz an diesem Zweck auszurichten und sich daran prüfen zu lassen.[77]

[77] Siehe Pohle (2015b).

Datenschutz zwingt Organisationen dazu, sich informationell nach außen abzuschotten und sich intern funktional zu differenzieren, verlangt also eine informationelle Gewaltenteilung. Organisationen sollen zerlegt werden in Teilorganisationen, die jeweils in der Lage sind, die Funktionen, die sie erfüllen sollen, auch zu erfüllen, dabei aber zugleich beschränkt sind auf ihre jeweiligen Funktionen – und damit in ihrer Macht. Diese Zerlegung kann real oder virtuell sein – relevant ist für den Datenschutz nur, dass sowohl die Organisations- wie auch die Teilsystemgrenzen als Informationsflussgrenzen wirken.

Der Datenschutz basiert auf dem gleichen Grundsatz wie das Rechtsstaatsprinzip, nämlich dass der Zweck nicht die Mittel heilige, und stellt daher Auswahl und Anwendung der Mittel unter Bedingungen. In maschinisierten und automationsgestützten Informationsverarbeitungs- und Entscheidungsfindungsverfahren lassen sich drei Komponenten analytisch trennen: Informationen, Prozesse und technische Systeme.

Informationen gelten aus Sicht des Datenschutzes als zentrale Machtmittel, denn sie sind die Rohstoffe für die Produktion von Entscheidungen. Zur Begrenzung der Organisationen in ihren Entscheidungsmöglichkeiten verlangt der Datenschutz eine funktionsorientierte Zuweisung von Informationen an Organisationen sowie gesteuerte Informationsflüsse in Organisationen, deren Regelung in Anlehnung an die Steuerung von Finanzmitteln teilweise als „Informationshaushalt“[78] bezeichnet wird. Darüber hinaus haben Organisationen funktionsdienliche Eigenschaften von Informationen zu garantieren, etwa Erforderlichkeit und Angemessenheit der Informationen für den festgelegten Zweck oder deren Korrektheit und Aktualität.

Die Informationsverarbeitungsprozesse, die der Entscheidungsfindung dienen, können beliebig komplex sein. Um sie dennoch unter Bedingungen stellen zu können, sollen sie, so der Operationalisierungsansatz des Datenschutzes, in Einzelschritte zerlegt werden, an die der Datenschutz dann konkrete, dem Bedrohungspotential des jeweiligen Schritts angemessene Anforderungen knüpfen kann. Der Datenschutz ging in seiner Entstehungszeit dabei einerseits von einer Typisierbarkeit dieser Einzelschritte aus und typisierte sie entsprechend, andererseits von der Vorstellung, dass, wenn in jedem einzelnen Verarbeitungsschritt alle Risiken unter Kontrolle gebracht und jede Bedrohung der Betroffenen und ihrer Rechte ausgeschlossen sind, eine Bedrohung insgesamt ausgeschlossen sei.[79]

Der Datenschutz hat ursprünglich darauf gesetzt, dass eine Regulierung der Informationsverarbeitungsprozesse in Verbindung mit dem Interesse der Organisationen an Rationalisierung, Maschinisierung und Automation dazu führen würde, dass die Organisationen Datenschutz aus eigenem Antrieb auch in Technik umsetzen würden. Dieser Ansatz wurde bereits direkt nach der Verabschiedung des BDSG 1977 hintertrieben – vom Bundesdatenschutzbeauftragten, einigen Landesdatenschutzbeauftragten, einigen Aufsichtsbehörden der Länder sowie interessierten Kreisen der Wirtschaft.[80] Mit Datenschutz by Design und by Default wird gegenwärtig ein neuer Versuch in dieser Richtung unternommen.

Schutz von Betroffenen kann nur von Organisationen garantiert werden, die sich selbst und ihre Mittel unter Kontrolle haben. Ausschließliche Eigenkontrolle bietet, wie in allen anderen durch Machtverhältnisse geprägten Lebensbereichen auch, dafür keine Garantie. Der Datenschutz setzt auf die Institutionalisierung einer grundsätzlich zweistufigen Kontrollstruktur, die selbst wieder auf der Eigenkontrolle der Organisationen aufsetzt. Datenschutz zwingt die Organisation dazu, ihre eigenen Verfahren unter Kontrolle zu bringen und kontrollfähig zu machen, um

[78] Siehe Müller (1975a, S. 123).
[79] Siehe Pohle (2014b, S. 89 ff.).
[80] Siehe Pohle (2015a).

nachzuweisen, dass die Verfahren alle Anforderungen erfüllen. Ab einer bestimmten Größe – oder Riskanz – der Organisation muss diese zusätzlich eine organisationsinterne, aber rollengetrennte Kontrollstruktur aufbauen. Auf der zweiten Ebene existiert eine externe Kontrollstruktur, die Datenschutzaufsichtsbehörden.

Wie vergleichbare Machtbeschränkungsansätze zwingt auch der Datenschutz die Macht zur Transparenz: Organisationen müssen ihre Zwecke, Strukturen und Verfahren offenlegen, sowohl den Betroffenen gegenüber als auch externen Aufsichtsorganen. In der Anfangszeit der Datenschutzdiskussion wurde darüber hinaus gefordert, dass auch die informationstechnischen Umsetzungen der Verfahren – die Programme – offengelegt werden müssen. Später bezog sich das nur noch auf den öffentlichen Bereich und verschwand dann für einige Zeit ganz von der Bildfläche. Inzwischen wird es als „Algorithmen"-Problem oder „Governance of Algorithms" wieder diskutiert. Hingegen ist die Forderung nach Transparenz der Modellannahmen inzwischen kein Thema mehr.

Auf der anderen Seite schafft der Datenschutz für die Betroffenen Möglichkeiten zur direkten Intervention in die Informationsverarbeitung der Organisationen. Prototypisch dafür steht etwa die bei der „informationellen Selbstbestimmung" überbetonte Kontrolle der Betroffenen über die Preisgabe von Informationen über sich selbst. Andere Interventionsmöglichkeiten sind das „Aufdrängen" von Informationen oder das Zum-Löschen-Zwingen.

3.4.4 Schlussfolgerungen

Der Datenschutz ist „konservativ", indem er die Ergebnisse vergangener gesellschaftlicher Aushandlungen zu seinem ersten Schutzgut erklärt. Er ist „fortschrittlich", indem er den gesellschaftlich konsentierten Modus der Veränderung dieser Ergebnisse zu seinem zweiten Schutzgut erklärt. Er schützt die Veränderbarkeit von Gesellschaft als Vorrecht der Gesellschaft gegen ihre einseitige Veränderung durch sozial, ökonomisch und politisch mächtige soziale Akteurinnen, deren Macht informationell begründet, vergrößert oder verfestigt wird.

Es wird dabei deutlich, wie sehr die Konstruktion des Datenschutzes bedingt ist durch die Annahmen über den Charakter von Organisation, Informationsverarbeitung und Technik. Datenschutz – genauer: dieses Modell von Datenschutz – ist eine angemessene Antwort auf das Machtproblem, das Bürokratien im Weberschen Sinne erzeugen. Fraglich ist, ob solche – idealtypischen – Bürokratien in der Realität existieren. Fraglich ist damit auch, ob dieses Modell von Datenschutz eine Antwort auf das Datenmachtproblem geben kann, das real existierende Organisationen erzeugen. Das Regelungsmodell des Datenschutzes ist jedenfalls so mechanistisch wie das Webersche Organisationsbild; es setzt im Grunde voraus, dass es der Organisation gelingt, die Herausbildung informeller Strukturen und Kommunikationsverbindungen in der Organisation zu verhindern oder zumindest dafür zu sorgen, dass sie sozial folgenlos bleiben, jedenfalls für die Betroffenen. Die dem Datenschutz zugrunde liegende Annahme, dass das Erforderlichkeitsprinzip zu einer Beschränkung der Informationsmenge – und mithin der Macht – in den Händen der Organisation führt, gilt allenfalls für kausalitätsbasierte Verfahren. In korrelationsbasierten Verfahren hingegen sind alle Informationen erforderlich, auch wenn sich vielleicht nachträglich herausstellt, dass sie nicht signifikant waren. Das Bild des Datenschutzes von der Erzeugung von Kontrollfähigkeit der Informationsverarbeitungprozesse ist tayloristisch und basiert auf der Annahme, dass die Zerlegung der Prozesse in Einzelschritte zugleich alle Probleme und Risiken in Teilprobleme und Teilrisiken zerlegen könnte, die sich dann innerhalb der Einzelschritte abschließend bannen ließen. Der Datenschutz stellt sich zuvorderst als Antwort auf einen instrumentellen Gebrauch von Technik und dessen Folgen dar. So angemessen die Antwort des

Datenschutzes auf diese Form von Gebrauch und dessen Folgen ist, sie bleibt tendenziell blind gegenüber den Folgen etwa eines performativen Gebrauchs von Technik oder der Tendenz zu totalen Mediatisierung. Die Möglichkeit zur Erzeugung von Transparenz ist vor allem deshalb substanziell beschränkt, weil sich das Transparenzverlangen des Datenschutzes inzwischen schon auf der abstrakten Ebene nicht mehr auf alle Elemente des Informationssystems bezieht. Und die Forderung nach Intervenierbarkeit griff schon immer zu kurz, wenn sie nicht auch auf von der Organisation nicht kontrollierbare Interventionen zielte, weil andernfalls der Erfolg jeder Intervention der Betroffenen von der Kooperation der Organisation abhängig bleibt.

Eine Alternative zu dem hier betrachteten mechanistischen Regelungsmodell des Datenschutzes könnte in der Verwendung von Schutzzielen bestehen, die dazu nicht wie bislang aus dem geltenden Datenschutzrecht, sondern direkt aus der Datenschutztheorie abgeleitet werden müssten.

3.5 Kritik des Datenschutzes und Rekonzeptionalisierungsansätze

Bei allen aufgedeckten Einzelproblemen ist zu konzedieren, dass die Datenschutzdiskussion der 1970er Jahre für die Rationalisierung, Mechanisierung und Automation der Informationsverarbeitung und der Entscheidungsfindung in Organisationen und deren gesellschaftliche Auswirkungen eine in Teilen sehr fundierte Analyse geliefert hat. In ihr spiegelt sich das große Interesse aller Beteiligten an einer interdisziplinären Zusammenarbeit wider und zugleich – jedenfalls in Bezug auf einige der für die Informatik zentralen Aspekte – auch deren Fähigkeit, die interdisziplinäre Anschlussfähigkeit tatsächlich herzustellen. Rückblickend hat die Datenschutzdiskussion mit dem Datenschutz einen Prototypen geliefert, an dem sich selbst einige der heutigen Debatten um *privacy*, Privatheit und Privatsphäre noch messen lassen können. Vor allem der verwendete Informationsbegriff und die Explikation des Modellierungsproblems stechen dabei heraus. Klar ist aber auch: Der Prototyp hätte ordentlich ausgetestet und dann verworfen werden müssen – so wie es auch für viele der Datenschutzgesetze in den 1970er Jahren geplant war. Aber genau das ist nie geschehen. Statt dessen ist das – im Gesetzgebungsverfahren schon weitgehend entkernte – Bundesdatenschutzgesetz einerseits in einer langen Folge von weitgehend selbstreferenziellen Novellierungen, andererseits vermittels der aus einander teilweise widersprechenden Architekturansätzen entstandenen EG-Datenschutzrichtlinie zu einem Gesetz geworden – und gemacht worden –, dessen einziges Ziel darin zu bestehen scheint, dafür zu sorgen, dass das Gesetz eingehalten wird. Eine fundierte Analyse des Prototyps hätte jedenfalls spätestens in den 1990er Jahren, nachdem die Organisationssoziologie einige neue Ansätze hervorgebracht hatte,[81] zu einem Nachdenken über eine mindestens teilweise, wenn nicht gar komplette Rekonzeptionalisierung führen müssen.

Die vorliegende Arbeit macht deutlich, dass der Datenschutz als „Lösung“ des durch die Industrialisierung der gesellschaftlichen Informationsverarbeitung erzeugten Datenmachtproblems in der Informationsgesellschaft des 21. Jahrhunderts – vor allem hinsichtlich der Informationsverarbeitung von Organisationen – neu abgeleitet werden muss. Dazu kann und sollte der Ableitungsprozess, der auch schon die historische Datenschutztheorie geprägt hat, verwendet werden. Dieser Prozess scheint selbst vor dem Hintergrund der Kritik an einigen seiner historischen Produkte immer noch weit besser geeignet zu sein als die oft zu findende simplifizierende Bezugnahme auf die Natur des Menschen, individuelle Befindlichkeiten, naturrechtlich begründete subjektive Rechte oder gar bereits bestehende Gesetze. Ausgangspunkt dieser Ableitung muss – wie schon

[81] Siehe Preisendörfer (2008, S. 21 f.).

in der historischen Datenschutzdiskussion – eine Analyse der gesellschaftlichen Informationsverarbeitung sein: Welche Eigenschaften haben die Akteurinnen – Organisationen, Individuen, Gruppen –, wie verarbeiten sie Informationen und treffen Entscheidungen, wie nutzen sie dabei Technik und welche; schließlich: Wie „nutzt" die Technik die Akteurinnen? Auf dieser Basis sind dann die Folgen dieser Informationsverarbeitungspraxen in vermachteten sozialen Beziehungen zu analysieren – und anschließend zu bewerten. Erst danach kann sinnvoll über „Lösungen" diskutiert werden.

Dabei wird vor allem deutlich, dass die Beschränkung der historischen Datenschutztheorie auf vermachtete Verhältnisse zugleich ein Befreiungsschlag für eine ordentliche Datenschutztheorie ist und bleibt. Nur so lässt sich nämlich sicherstellen, dass die Datenschutztheorie nicht schon versucht, eine umfassende Theorie der Informationsgesellschaft zu werden, oder dass bei der Verwendung von personenbezogenen oder sonstigen Informationen als Anknüpfungspunkt einer Analyse oder einer Theorie nicht verhindert werden kann, dass sich eine untere Grenze des Anwendungsbereiches schon strukturell nicht finden lässt, weil klar ist: Soziale Akteurinnen können nicht nicht Informationen verarbeiten.[82]

Während also der Ableitungsprozess ein besonders herausragendes Ergebnis dieses Teils der Datenschutzdiskussion ist, muss die dort vorgelegte Dokumentation der Datenschutztheorie hingegen als besonders mangelhaft eingeschätzt werden. Es ist in der ganzen Debatte keiner der Vertreterinnen gelungen, eine umfassende und doch lesbare Darstellung der Datenschutztheorie mit ihren Annahmen, ihrer Beschreibung und Analyse der Auswirkungen der modernen Informationsverarbeitung auf Individuen, Gruppen und die Gesellschaft, aber auch auf andere Organisationen und das staatliche Institutionengefüge insgesamt, sowie einem vorgeschlagenen Regelungsregime und dessen Begründung vorzulegen.

3.5.1 Angreifermodell

Auch wenn Organisationen nicht unbesehen und in ihrer Gesamtheit als rational oder im Weberschen Sinne zweckrational imaginiert werden dürfen, stellt doch der Topos der Rationalität immer noch einen wesentlichen Bezugspunkt des Organisationsverständnisses verschiedener Disziplinen und Schulen, der Selbstbeschreibung von Organisationen und der Organisationsberatung dar.[83] Auch Zwecke haben als Bezugspunkt nicht ausgedient, auch wenn sie heute eher als Ziele bezeichnet werden.[84] Klar ist auch, dass Organisationen versuchen, ihre Informationsverarbeitung möglichst weitgehend zu rationalisieren, zu automatisieren und zu industrialisieren, um ihre Entscheidungsfindung zu verbessern[85] – und dabei nicht immer erfolgreich sind.[86] Dabei werden die Bedingungen sehr weitgehend von der Organisation selbst bestimmt: Sie legt grundsätzlich

[82] Vergl. für Kommunikation Watzlawick et al. (1967, S. 48 ff.), die zugleich, so Luhmann (2000, S. 57), Informationsverarbeitung ist.

[83] Siehe dazu etwa Preisendörfer (2008, S. 17 ff., 95 ff.), Abraham und Büschges (2009, S. 19 ff.) und Kühl (2011, S. 28 f.).

[84] So Abraham und Büschges (2009, S. 39, Fn. 24.). Siehe umfassend Preisendörfer (2008, S. 62 ff.).

[85] Siehe etwa für den Bankensektor Riese (2006).

[86] Hier ist allerdings einschränkend darauf hinzuweisen, dass das, was Organisationen (noch) als Erfolg ansehen, aus der Sicht des betroffenen Klientels durchaus ganz anders darstellen kann, siehe etwa die Rubrik „Vorsicht, Kunde" in der c't, in der in steter Regelmäßigkeit die entstandenen Probleme als Folgen der Automatisierung von Verfahren markiert werden – sowohl in den Antworten der Unternehmen als auch durch die Autorinnen: Die Tatsache, dass „[k]omplett durchrationalisierte Organisationen [...] zunehmend unflexibel [reagieren], wenn sich bei weitgehend automatisierten Abläufen Störungen einstellen", Mansmann (2016, S. 75), stellt jedoch im Zweifel nur aus Sicht der Kundinnen einen Misserfolg dar.

ihre eigenen Modellannahmen zugrunde, gestaltet die Informationsverarbeitungs- und Entscheidungsverfahren nach ihren eigenen Interessen und entscheidet selbst, welche Informationen sie in welcher Form intern abbildet und zur Entscheidungsfindung heranzieht.[87] Gleiches gilt für die innerhalb von Organisationen – etwa aus Korrelationsanalysen – erzeugten Informationen, die von der Organisation im Anschluss selbst wieder als Prämisse und Produktionsmittel für weitere Entscheidungen eingesetzt werden. Die Modellierungshoheit der Organisation bezieht sich aber nicht nur auf die Informationen und Informationsverarbeitungsprozesse, sondern grundsätzlich auch auf die technischen Systeme, die die Organisation einsetzt. Das gilt in jedem Fall für die Auswahl der Systeme, wenn auch nicht zwangsläufig zugleich für deren Gestaltung. Mit den von der Organisation eingekauften oder angemieteten Systemen importiert diese oft zugleich organisationsfremde Modellannahmen und -logiken, auch wenn die damit einhergehende relative Fremdbestimmung durch die Konfigurationshoheit der Organisation abgemildert wird.

Innerhalb von Organisationen herrscht noch immer ein instrumentelles Verständnis von Technik vor, genauso wie auch davon ausgegangen werden kann, dass Organisationen versuchen, sich die von ihr eingesetzte Technik nach ihren eigenen Interessen und für ihre eigenen Ziele oder Zwecke als Instrument zu gestalten. Zugleich wird aber die Technik weder von organisationsinternen noch von organisationsexternen Akteurinnen ausschließlich instrumentell eingesetzt:[88] Sie wird entdeckt, sich angeeignet, fehlgenutzt, umgenutzt, zweckentfremdet, gehackt, bespielt, nicht wahrgenommen, demonstriert, konsumiert oder schlicht ignoriert – und durchaus auch alles gleichzeitig. Dass das gleiche System für unterschiedliche Nutzerinnen ganz unterschiedliche Rollen spielen und ganz unterschiedlich genutzt werden kann, bezieht sich dabei nicht nur auf die Zwecke, die diese Akteurinnen verfolgen.[89] Es bezieht sich, wie das Beispiel der sozialen Netzwerke zeigt, auf das gesamte Verhältnis zwischen Nutzerinnen und Technik: Für die Nutzerinnen des sozialen Netzwerks ist das technische System vor allem Informations- und Kommunikationsmedium, für die Betreiberin hingegen in erster Linie ein klassisches Instrument – für die Aufrechterhaltung des Betriebs, für die Beobachtung des Verhaltens und der Kommunikation der Nutzerinnen sowie für deren ökonomische Verwertung. Dabei können sowohl die Akteurinnen als auch ihre jeweiligen Rollen für jeweils andere Akteurinnen sehr unterschiedlich sichtbar sein, wobei manche Akteurinnen erst sichtbar werden, wenn es zu unerwünschten Nebenwirkungen kommt oder die Technik ausfällt.[90] Zugleich kann nicht mehr unterstellt werden, dass die Organisation ihre eigene Technik durchgängig versteht oder gar beherrscht. Gerade die weitverbreitete Nutzung von Standardsoftware oder Software-as-a-Service weist darauf hin, dass auch für die Organisation selbst wesentliche Eigenschaften – und damit sowohl Wirkungen wie Nebenwirkungen – tendenziell unsichtbar bleiben.

[87] Siehe dazu Luhmann (2000, S. 36, 49 und vor allem 51 f.), der Organisationen daher als autopoietische Systeme bezeichnet, denn sie seien „*operativ geschlossen* und in genau diesem Sinne *autonom*“ (S. 51, Hervorhebung im Original). Ausnahmen von der weitgehenden organisationseigenen Autonomie gibt es – jedenfalls mittelbar – dort, wo die Organisation Modellannahmen, Verfahren oder Daten übernimmt; das in der Informatik-Diskussion bekannteste Beispiel ist das Vorgehen von SAP, die ihre Unternehmenskundinnen „überzeugt“, die SAP-eigenen Vorstellungen zu übernehmen, um SAP-Systeme sinnvoll einsetzen zu können.

[88] Siehe etwa Rammert (2007, S. 11 ff.).

[89] Siehe etwa Steinmüller (1981, S. 184) zur Multifunktionalität von Informationssystemen: „Besonders deutlich wird es an einem »harmlosen« maschinisierten Zeitungsausschnittdienst namens »Pressedatenbank« und seinen Benutzern: Je nach Verwertern ist das gleiche System Dokumentationssystem zur Erleichterung der journalistischen Arbeit, Managementinformationssystem zur Auswahl künftiger oder Personalinformationssystem zur Beurteilung (und ggfs. Freistellung) gegenwärtiger Mitarbeiter, schließlich Polizeiinformationssystem, etwa über »Radikale« aller Arten: Alle diese Informationen können binnen Sekunden herausgesucht (»gerastert«) werden.“

[90] So etwa Rammert (2007, S. 13 f.).

Ein für die Gestaltung von Technik brauchbares Datenschutz-Angreifermodell muss alle diese Aspekte anwendungsbereichsspezifisch konkretisieren. Vor dem Hintergrund, dass sich die tatsächlichen Auswirkungen von Angreiferinnen auf Individuen, Gruppen, Organisationen und die Gesellschaft nur einschätzen lassen, wenn das Informationssystem möglichst weitgehend bekannt ist und der Analyse zugrunde gelegt wird,[91] kann ein abstraktes Modell, wie es hier beschrieben wurde, nur der Ausgangspunkt für eine Konkretisierung sein, nicht aber schon die Grundlage für eine Bedrohungsanalyse, die mehr bietet als allgemeine Hinweise auf grundlegende Problembereiche. Dazu gehören der konkrete Anwendungsbereich des zu gestaltenden – oder des zu prüfenden – Systems und die beteiligten oder zu beteiligenden Akteurinnen, ihre konkreten Rollen und gesellschaftlich geprägten Erwartungen, ihre Interessen, Rechte und Pflichten, ihre Ziele und Zwecke, ihr jeweiliges Verhältnis zueinander, vor allem ihr Machtverhältnis, sowie ihre tatsächliche Kontrolle – oder ihr Kontrolldefizit – über die und ihr konkreter Umgang mit den informationstechnischen Systemen.

3.5.2 Bedrohungsmodell

Auf dieser Basis kann dann eine anwendungsbereichsspezifische Bedrohungsanalyse durchgeführt und ein angemessenes Bedrohungsmodell generiert werden, das als Grundlage sowohl für rechtliche Regelungen als auch für die Gestaltung und den Einsatz informationstechnischer Systeme dienen kann.[92] Das im Folgenden dargestellte analytische Raster für die Bedrohungsanalyse wird hingegen wegen des Verzichts auf eine Anwendungsbereichsspezifizierung nur die grundlegenden Problembereiche umreißen.

Im Bedrohungsmodell werden die Auswirkungen des Informationsgebarens von informationsverarbeitenden Organisationen auf ihre Umwelt problematisiert. Als zur Umwelt gehörend werden sowohl Individuen und Gruppen (Individualdatenschutz) sowie Organisationen und Institutionen (Institutionaldatenschutz) verstanden, soweit sie jeweils Betroffene sind, weil Informationen über sie verarbeitet oder Entscheidungen über sie getroffen werden, weil sie die von den Organisationen entwickelten oder ausgewählten informationstechnischen Systeme einsetzen oder weil ihre gesellschaftlich konsentierten Interessen berührt sind, sowie alle gesellschaftlichen Akteurinnen und die Gesellschaft als Ganzes (Systemdatenschutz), soweit das Informationsverhalten der Organisationen sozialschädliche Folgen herbeiführen kann.[93] Die gesellschaftlich konsentierten Interessen sind in erster Linie die Freiheits- und Partizipationsversprechen der modernen bürgerlichen Gesellschaft,[94] genauso aber die Strukturschutzprinzipien und -mechanismen der

[91] Siehe Steinmüller (1993, S. 222).

[92] Oder, in der Beschreibung des Datenschutzes aus der Sicht Steinmüllers: „Der Grundgedanke des Datenschutzes ist »systemanalytisch« (und gerade nicht juristisch, wie selbst Juristen und Informatiker mißverstehen)“, Steinmüller (1993, S. 625).

[93] Siehe zu Individual- und Institutionaldatenschutz – oder auch Datenschutz im engeren und im weiteren Sinne – Steinmüller et al. (1971, S. 44) und zum Systemdatenschutz Podlech (1982, S. 451 f.). Die meisten der nachfolgend angegebenen Quellen beschränken sich in der Analyse der Bedrohungen ausschließlich auf Individuen als Betroffene. Selbst in diesen Fällen ist jedoch oft eine Übertragung auf alle sozialen Akteurinnen und die Gesellschaft insgesamt möglich.

[94] Im Gegensatz zur herrschenden Meinung unter den Juristinnen sind damit nicht nur die verfassungsrechtlich garantierten „Grundrechte und Grundfreiheiten“ (Art. 1 Abs. 2 EU-DSGVO) – oder gar nur, wie § 1 Abs. 1 BDSG ausweist, das Persönlichkeitsrecht – gemeint, denn mit diesen historisch als Schutz- und Abwehrrechte gegen den Staat entstandenen Rechten können nur Akteurskonstellationen in den Blick genommen werden, in denen der Staat einer der unmittelbar oder mittelbar beteiligten Akteurinnen ist – oder irgendwann in der Vergangenheit war, wie etwa als Anbieter von Telekommunikationsdiensten (Reichspost, Bundespost). Konstellationen, an denen der Staat nie beteiligt war oder in denen gerade nicht das Verhältnis Bürgerin–Staat

verfassungsmäßigen Ordnung. Betroffene stellen dabei selten oder nie eine homogene Gruppe dar, Betroffene können also in sehr unterschiedlicher Weise und in sehr unterschiedlichem Umfang betroffen sein.[95]

Das allgemeine Datenmachtproblem[96] entsteht, weil informationstechnische Systeme und die durch sie mitkonstituierten soziotechnischen Informationssysteme als „Machtverstärker" wirken:[97] Sie verstärken die Möglichkeiten der Akteurinnen – im Datenschutzbereich: der Organisationen –, die Kontrolle über diese Systeme haben – oder genauer: über die Leistungen der Systeme verfügen können –, zur Steuerung oder Beeinflussung individueller, kollektiver oder institutioneller Betroffener und ihrer Kommunikationen, Entscheidungen und Handlungen sowie der Prästrukturierung ihrer Handlungsmöglichkeiten.[98] Das allgemeine Datenmachtproblem ist eine direkte Folge – und aus Sicht der Organisationen eine *gewünschte* Folge – der durch Rationalisierung, Maschinisierung und Automation verbesserten Informationsverarbeitungs- und Entscheidungsfähigkeiten von Organisationen. Welche zu problematisierenden Machtverschiebungen sich dabei tatsächlich ergeben, hängt sowohl vom konkreten soziotechnischen Informationssystem wie auch von seiner spezifischen Umwelt ab. Erst auf der Basis einer Analyse der konkreten Machtverschiebung kann entschieden werden, ob diese gesellschaftlich akzeptabel oder gar erwünscht ist oder nicht.[99]

Neben dem allgemeinen Datenmachtproblem als Folge moderner Informationsverarbeitung als solcher erzeugt die konkrete Gestaltung, Organisation und Ausführung von Informationsverarbeitung und Entscheidungsfindung Probleme auf verschiedenen, analytisch voneinander zu trennenden Ebenen. Grundlegender Anknüpfungspunkt für eine Analyse dieser Probleme ist das Verfahren, das mit seinen Bestandteilen Informationen, Prozesse und informationstechnische Systeme[100] dem entspricht, was in Organisationslehre und Informatik als Geschäftsprozess oder *use case* bezeichnet wird, und das dem Erreichen eines von der Organisation gesetzten Zweckes dient.[101]

Das umfassendste, weil sich auf alle Verfahrensbestandteile erstreckende Problem stellt die schon beschriebene Rationalitätsverschiebung dar, die sich daraus ergibt, dass Organisationen alle Objekte aus ihrer Umwelt auf der Basis von Modellannahmen, die unter Modellierungshoheit

adressiert wurde, etwa im Bereich des Mietrechts oder des Verbraucherinnenschutzes, müssten bei einer solchen Selbstbeschränkung notwendig im Dunkel bleiben. Schon die grundrechtsgleichen Rechte werden gemeinhin ignoriert, siehe Garstka (1977) oder Gallwas (1979). Diese Konstellationen sind darum aber nicht weniger vermachtet und daher riskant für die Rechte und Freiheiten der Betroffenen.

[95] Siehe dazu Raab und Bennett (1998).

[96] Siehe zu Fragen der Datenmacht grundlegend sowie in verschiedenen Bereichen und in verschiedenen Ausprägungen Scheuch (1974), Schmidt (1974), Weizenbaum (1976), Steinmüller (1979b), Lenk (1982), Simitis (1987), Zuboff (1988), Steinmüller (1993), Solove (2001), von Lewinski (2009), Tække (2011), Rost (2013b), Newman (2014) und Caplan und boyd (2016).

[97] Siehe Steinmüller (1993, S. 417).

[98] Dieses Datenmachtproblem ist nicht nur, wie es vielleicht scheinen könnte, Folge der Nutzung von Informationen durch Organisationen, sondern kann auf Betroffene schon qua Existenz des Informationssystems wirken. Siehe für eine frühe Analyse des Problems solcher „chilling effects" White und Zimbardo (1975) sowie BVerfG (1983, S. 43): „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten."

[99] Ein Beispiel für klar gesellschaftlich erwünschte Machtverschiebungen ist das Ergebnis der Einführung von Transparenzpflichten: Solche Pflichten werden gerade gefordert, *um Machtverschiebungen auszulösen.*

[100] Siehe dazu Bock und Meissner (2012).

[101] Siehe Pohle (2014b, S. 89 f., Rn. 10).

der Organisationen nach organisationseigenen Zwecken[102] produziert werden, intern abbilden, der organisationseigenen Funktions- und Verfahrenslogik unterwerfen und nach organisationseigenen Programmen verarbeiten.[103] Informationsverarbeitung auf der Basis von Modellannahmen und Auswahlentscheidungen,[104] Entscheidungsprämissen und Entscheidungsprogrammen[105] reproduziert die diesen zugrunde liegenden – oder zugrunde gelegten – Verzerrungen.[106] Am wirkmächtigsten zeigt sich die Rationalitätsverschiebung im Zuge der Automatisierung von Verfahren,[107] weil Technik, vor allem IT, als geronnene Organisation an die Stelle der Organisation selbst tritt,[108] mit der Betroffene im Zweifel noch verhandeln könnten.

In das Analyseraster für die Bedrohungsanalyse fallen grundsätzlich alle Informationen, die für die Entscheidungsfindung genutzt werden können, nicht nur für Entscheidungen über Menschen[109] und nicht nur personenbezogene Informationen.[110] Es geht um sozial wirksame Entscheidungen und mithin um die diesen zugrunde liegenden Informationen. Das zentrale Problem im Hinblick auf Informationen sind die Ketten von Verdatungen und Reinterpretationen, also Transformationen von Informationen – mit den Dimensionen Syntax, Semantik, Pragmatik und Sigmatik – in Daten, die nur Zeichen oder Zeichenketten sind, und von Daten in Informationen, die im Allgemeinen nicht verlustfrei durchgeführt werden können.[111] Zu prüfen ist für ein konkretes Informationssystem an dieser Stelle, zu wessen Nachteil sich diese Verluste auswirken. Gleiches gilt für die Frage nach der Korrektheit von Informationen: Es ist immer zu prüfen, ob „»richtige« oder »falsche« [Informationen] »nützlicher« oder »gefährlicher« für Interessenten und Betroffene sind."[112]

Die Bedrohungsanalyse nimmt die Prozesse sowohl in ihrer Gesamtheit als auch ihre einzelnen Phasen in den Blick.[113] Als Phasen werden dabei – wie bei Steinmüller et al.[114] – die einzelnen typisierten, regelmäßig wiederkehrenden Zustände von Informationsverarbeitungsprozessen verstanden, die zugleich als analytisches Raster wie als Ansatzpunkt für die Problemlösung dienen.[115] Für ihre Verwendung als Analyseraster gilt dabei, dass sie nicht exkludierend sind: Nicht

[102] Auch Zweckfreiheit ist ein Zweck in diesem Sinne, gerade weil Organisationen ein Interesse daran haben können, den Zweck offen zu lassen. Aus der Sicht der statistischen Informationstheorie verringert Information – also Entscheidung – Freiheit, so Steinbuch (1980, S. 15). Im Fall der Entscheidung für einen Zweck heißt das konkret, dass eine – aus Organisationssicht – zu frühe Entscheidung die Optionen für mögliche Entscheidungen in der Zukunft einengt. Das erklärt zugleich, warum Zwecksetzung – sowohl als Fremd- wie als Selbstbindung –, gerade weil sie die Freiheit der Organisation beschränkt, zusammen mit der Zweckbindung ein derart zentrales Instrument des Datenschutzes und des Datenschutzrechts ist, siehe Pohle (2015b).

[103] Siehe dazu umfassend Pohle (2016c).

[104] Siehe Harbordt (1975, S. 72 ff.).

[105] Siehe Luhmann (2000, S. 222 ff., 256 ff.).

[106] Siehe umfassend Barocas und Selbst (2015).

[107] Siehe schon Podlech (1982, S. 460).

[108] Siehe Lenk (2016, S. 354).

[109] So schon für Planungsinformationssysteme Dammann (1975), siehe auch allgemein unter dem Label „Informationsschutz" Steinmüller (1993, S. 676 ff.).

[110] So schon unter dem Label „personenbezogene (auf die natürliche Person des Bürgers bezogene) Interessen an Daten" Rihaczek (1980, S. 229).

[111] Jedenfalls immer dann nicht, wenn es nicht eine vordefinierte eindeutige Interpretationsregel gebe, so Brunnstein (1975, S. 156).

[112] Siehe Steinmüller (1975a, S. 521, Fn. 36).

[113] Zur Forderung nach einem solchen post-tayloristischen Analyseansatz siehe Pohle (2016c, S. 9).

[114] Siehe Steinmüller et al. (1971, S. 57).

[115] „Da diese Schritte bei jeder IV [Informationsverarbeitung] typisch wiederkehren (mögen auch gelegentlich einzelne Phasen ausfallen), haben sie grundlegende Bedeutung: in ihnen werden die Individualinformationen verarbeitet mit je spezifischen Auswirkungen und Gefährdungen für den Betroffenen", so Steinmüller et al. (1971, S. 57). Das Konzept der Phasenorientierung ist, obwohl es dem deutschen Datenschutzrecht bis heute

nur können sie einzeln oder in beliebigen Kombinationen nacheinander auftreten, ein konkreter Informationsverarbeitungsschritt kann auch mehr als eine Phase umfassen.

Der Bedrohungsanalyse werden folgende Phasen zugrunde gelegt: Erheben, Speichern, Verändern – mit den herausgehobenen Subtypen Sperren, Pseudonymisieren und Anonymisieren –, Erzeugen, Übermitteln, Nutzen und Löschen.[116] Als Oberbegriff für jede Art des Umgangs mit Informationen soll Verarbeiten dienen – Verarbeiten ist damit mehr als die Summe der nachfolgenden Phasen.[117] Erheben bezeichnet dann den Prozessschritt, durch den Informationen oder Daten in den Herrschaftsbereich der Organisation gelangt.[118] Speichern bezeichnet die Verstetigung von Informationen, also die Herstellung und Aufrechterhaltung der Möglichkeit – zeitlich – späterer Reproduzierbarkeit, vor allem zur weiteren Verarbeitung. Verändern ist dann jede Transformation von Informationen, die die semantische, pragmatische oder sigmatische Dimen-

zugrunde liegt, extrem untertheoretisiert. Abgesehen von den drei Seiten bei Steinmüller et al. (1971, S. 57–59) und den Ausführungen bei Steinmüller (1993, S. 225 ff.) lässt sich in der deutschsprachigen rechtswissenschaftlichen Literatur keine Auseinandersetzung mit dem Konzept der Phasenorientierung finden. Die Phasen werden ausschließlich als Anknüpfungspunkte für das Recht behandelt, siehe etwa Simitis (Dammann in: 2011, § 3, Rn. 100 ff., 111 ff.), oder – in sehr wenigen Fällen – für die Technikgestaltung, siehe etwa Bräutigam et al. (1990, S. 59 ff.). Auch die Hinzunahme von „Erhebung“ und „Nutzung“ in den Kreis der gesetzlich geregelten Phasen infolge der Entscheidung des BVerfG zum Volkszählungsgesetz, siehe Zilkens (2008, S. 103 f., Rn. 68), hat nichts daran ändern können. Den gesetzlich definierten Phasen, siehe etwa § 3 BDSG, mangelt es damit an einer wissenschaftlich fundierten Begründung, vor allem hinsichtlich ihrer Geeignetheit als Analyseinstrumente. Eine solche Begründung, so notwendig sie wäre, liegt aber – vor allem aus Platzgründen – auch außerhalb des Rahmens der vorliegenden Arbeit.

[116] Diese Typisierung folgt im Ansatz der von Steinmüller et al. (1971, S. 57) vorgelegten und im Laufe der Zeit in veränderter Form im BDSG abgebildete Einteilung, ohne allerdings deren Beschreibungen unbesehen zu übernehmen, und ergänzt sie um die Phase „Erzeugen“, die Steinmüller (1993, S. 230) ohne Erklärung oder Begründung unter „Erheben“ fasst. Zwar problematisiert das BDSG an einer Stelle – in § 3 Abs. 4 Satz 2 Nr. 3 2. Alternative – schon aus gespeicherten Informationen erzeugte – „gewonnene“ – Informationen, und auch in der Literatur wird das Erzeugen verschiedentlich adressiert, historisch vor allem unter den Begriffen „Vorhersage“ oder „Planungsinstrument“, siehe etwa Steinmüller et al. (1971, S. 39 f.), in den 1990er Jahren mit „Profiling“ oder „Data Mining“, siehe etwa Clarke (1993), und heute mit „predictive analytics“ oder „Big Data“, siehe etwa Crawford und Schultz (2014). Während es bei den anderen Phasen an einer ordentlichen analytischen Durchdringung mangelt, fehlt es in Bezug auf die Phase „Erzeugen“ nicht nur an einem begrifflichen Bezugspunkt, sondern vor allem an einer Umsetzung im Recht. Die neben dem Gutachten „Grundfragen des Datenschutzes“ einzige andere Arbeit, die sich für eine Bedrohungsanalyse einer solchen Typologie von Informationsverarbeitungsschritten bedient, siehe Solove (2006), bietet mit den Phasen „(1) information collection, (2) information processing, (3) information dissemination, and (4) invasion“ (S. 488) keine der Komplexität moderner Informationsverarbeitung adäquate Anknüpfbarkeit. Gleiches gilt für die EU-DSGVO, die in Art. 4 Nr. 2 unter Verarbeitung „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ fasst, damit allerdings gerade nicht auf eine phasenorientierte Analyse zielt und im Übrigen diese „Vorgänge“ nicht einmal konsequent als Anknüpfungspunkte für rechtliche Anforderungen verwendet.

[117] Im Gegensatz zum BDSG ist damit Verarbeiten und nicht Nutzen die Auffangphase, siehe etwa Däubler et al. (Weichert in: 2010, § 3, Rn. 45).

[118] Das von der h. M. offensichtlich geforderte „aktive“ Element, siehe Simitis (Dammann in: 2011, § 3, Rn. 104), ist für die Bedrohungsanalyse nicht nur irrelevant, sondern geht schon am Begriff der „Gefährdung“ vorbei, um den sich doch das Datenschutzrecht drehe, siehe Simitis (Simitis in: 2011, § 1, Rn. 79). Für die Zurechnung auf die Organisation ist es dabei gleich, ob die Organisation selbst oder durch ihre Mitarbeiterinnen handelt. Die Fehlzuweisung ist eine Folge des weitverbreiteten methodologischen Individualismus, wonach zur Erklärung organisatorischer Phänomene immer am Verhalten der Individuen angesetzt werden müsse, da Individuen handeln könnten, nicht jedoch Institutionen oder Organisationen.

sion beeinflusst.[119] Sperren ist dann das Verändern von Informationen derart, dass sie zwar noch für die Organisation grundsätzlich nutzbar bleiben, jedoch nicht mehr für bestimmte Teile der Organisation zu bestimmten Zwecken.[120] Ähnlich ist die Definition von Pseudonymisieren: das Verändern von Informationen derart, dass sie für bestimmte Organisationsteile nicht mehr auf die konkreten sozialen Akteurinnen bezogen werden können, auf die sie für die Organisation als Ganzes noch beziehbar sind.[121] Hingegen verhindert Anonymisieren die begründbare Beziehung von Informationen auf konkrete soziale Akteurinnen auch für die Organisation.[122] Das Erzeugen von Informationen ist der Verarbeitungsschritt, mit dem neue, vorher nicht vorhandene – und auch nicht anders vorhandene oder bei einer anderen Akteurin vorhandene – Informationen geschaffen oder gewonnen werden.[123] Übermitteln bezeichnet, in Anlehnung an die Definition von Erheben, den Prozessschritt, durch den Informationen oder Daten in den Herrschaftsbereich Dritter – also nicht der Organisation selbst oder der Verdateten – gelangen soll, unabhängig vom Erfolg. Dritte können dabei Personen außerhalb der Organisation, andere Organisationen oder die Öffentlichkeit sein. Nutzen ist jedes zweckgerichtete Gebrauchen oder Verwenden von Informationen. Und Löschen ist – im Verhältnis zu Sperren sehr ähnlich wie das Verhältnis zwischen Anonymisieren und Pseudonymisieren – das Unkenntlichmachen von Informationen derart, dass sie auch für die Organisation nicht mehr nutzbar sind.

Neben die schon angesprochenen Risiken, die sich auf alle Verfahrensbestandteile – und damit auch auf die Prozesse – beziehen, wie die Rationalitätsverschiebung, treten die verarbeitungs- oder prozessspezifischen. Beim zentralen phasenübergreifenden Problem handelt es sich um eines der IT-Sicherheit – das Problem der Nichtabschottung des Informationssystems und des nichtausgeschlossenen undichten Dritten,[124] das in beide Richtungen wirken kann. Nicht nur

[119] Eine inhaltliche Änderung ist unstreitig eine Veränderung im datenschutzrechtlichen Sinne, siehe Simitis (Dammann in: 2011, § 3, Rn. 129). Hingegen ist durchaus umstritten, ob Änderungen der pragmatischen oder der sigmatischen Dimension sowie das Löschen als Verändern im Rechtssinne gelten, vergl. Däubler et al. (Weichert in: 2010, § 3, Rn. 35). Nur Steinmüller (1993, S. 200) fasst explizit Zweckänderung als Informationsveränderung. Wenn Erheben und Speichern nicht als Verändern gelten sollen, so in der Konsequenz etwa Simitis (Dammann in: 2011, § 3, Rn. 141 f.), obwohl es den informationellen Zustand der Organisation ändert, dann wohl auch nicht Löschen. Das Problem – aber eben auch die Möglichkeiten zu seiner Lösung – einer mangelhaften Konzeptionalisierung der Phasenorientierung zeigt sich etwa in der Entscheidung des BVerfG im BKAG-Urteil, die „hypothetische Datenneuerhebung“ zur verfassungsrechtlich gebotenen Operationalisierung des Zweckbindungsgrundsatzes für Fälle zweckfremder Nutzung von Informationen zu erklären, siehe BVerfG, Urteil des Ersten Senats vom 20. April 2016 – 1 BvR 966/09 – Rn. 287.

[120] Um Sperren handelt es sich dabei nur, wenn die Informationen für diese Organisationsteile faktisch nicht nutzbar sind, nicht jedoch, wenn die Nutzung nur für nicht erlaubt erklärt wird – egal ob per Anweisung oder durch Markierung der Informationen als „gesperrt“.

[121] Hierbei handelt es sich – wie im Folgenden auch für das Anonymisieren – um eine Anpassung an die Tatsache, dass als Betroffene nicht allein Personen in den Blick genommen werden.

[122] Die Tatsache, dass Organisationen auch anonyme oder gar Sachinformationen auf soziale Akteure beziehen können, etwa qua Zuschreibung, siehe Pohle (2016c, S. 11), oder indem sie darauf ihre Entscheidungen über diese Akteurinnen basiert, siehe Pohle (2016b, S. 15), ist keine Verletzung der Definition, sondern zeigt nur, dass die Fixierung auf Personenbezug für die Bedrohungsanalyse ebenso wie für die rechtliche Regelung ungeeignet ist.

[123] Der Begriff des Erzeugens ist damit enger, als ein konstruktivistisches Herangehen nahelegen würde, nach dem Informationen nicht von Organisationen übernommen, sondern immer nur intern erzeugt werden, siehe Luhmann (2000, S. 52 f.) und Heylighen und Joslyn (2001); darauf bezieht sich vielleicht auch die Einordnung bei Steinmüller (1993, S. 230). Auch Entscheiden stellt grundsätzlich noch kein Erzeugen im Sinne der hier vorgelegten Definition dar – siehe aber Steinmüller (1993, S. 244) –, es sei denn, die Produkte der Entscheidungen sollen als Basis für zukünftige Entscheidungen in verselbständigter Form dienen, nämlich gerade als neue Informationen.

[124] Siehe schon Steinmüller et al. (1978, S. 98 f.).

lassen sich für solcherart „offene“ Systeme keine konkreten Bedrohungsanalysen erstellen, die informationsverarbeitende Organisation kann auch keine Eigenschaften über die Nutzung des Informationssystems durch Dritte oder die weitere Verwendung oder Verbreitung der Informationen garantieren. Nichtabschottung ist insofern einerseits gleichbedeutend mit Veröffentlichung, andererseits mit einem von beliebigen Akteurinnen nutzbaren System. Ein zweites Problem, das sich auf alle Phasen erstreckt, liegt in der tendenziellen Intransparenz der Informationsverarbeitungsprozesse zum Nachteil der Betroffenen.[125] Auch auf alle Phasen, genauso aber auch phasenübergreifend wirken sich Verfestigungstendenzen aus, die sich etwa schon bei der Formalisierung und Rationalisierung von Prozessen, vor allem aber bei ihrer Automatisierung zeigen – die Prozesse können also tendenziell nur noch so, wie von der Organisation gestaltet, aber nicht mehr anders durchgeführt werden.[126] Der damit einhergehende Kontingenzverlust verringert nicht nur die Fähigkeit von Organisationen, flexibel – und damit situations-, ereignis- oder betroffenenangemessen – reagieren zu können, sondern verringert auch die Möglichkeit von Betroffenen, Einfluss auf die Organisation und deren Prozesse zu nehmen – und mithin auf deren Entscheidungen.[127] Es droht damit sowohl ein Selbst- wie ein Mitbestimmungsverlust, aber auch die schon angesprochene tendenzielle Verschlechterung der Rechtspositionen der Betroffenen.[128]

Die phasenspezifische Risiken beim Erheben von Informationen folgen schon aus der Wahl der Quelle durch die Organisation. So führt eine Erhebung bei Dritten zu einer doppelten Fremddefinition und mithin Fremdbestimmung der Betroffenen – einerseits durch die Dritten, andererseits durch die Organisation –, während die Erhebung von Informationen über Betroffene aus verschiedenen Kontexten, gesellschaftlichen Subsystemen oder Lebensbereichen das schon angesprochene Risiko der gesellschaftlichen Entdifferenzierung birgt und zugleich individuelle oder kollektive Strategien zu Rollen-, Kontext- oder Logiktrennung unterläuft[129] – mit der Folge möglicher, gesellschaftlich inakzeptabler Koppelung.[130] Aus der grundsätzlich einseitig ausgeübten Kontrolle der Organisation über die Erhebung erwächst auch das Risiko, dass die Organisation Informationen erhebt, die – mindestens aus der Sicht der Betroffenen – falsch, einseitig oder unpassend, weil in keinem Zusammenhang mit den Betroffenen, den vermeintlich abgebildeten Ereignissen oder Sachverhalten oder mit den zu treffenden Entscheidungen, sind. Ein weiteres Risiko, das aus dieser Kontrolle über die Erhebungsbedingungen erwächst, besteht in der gegen die Interessen der Betroffenen gerichteten Verweigerung von Organisationen, bestimmte Informationen zu erheben.[131] Und nicht zuletzt sind es bestimmte Formen der Erhebung, etwa die Massenüberwachung durch Geheimdienste oder eine heimliche Beobachtung, oder bestimmte Mittel, etwa Gewalt oder gar Folter, die als Bedrohungen im Rahmen dieser Phase identifiziert werden können.

[125] Zu den Folgen siehe etwa Müller und Kuhlmann (1972) oder Koops (2013). Darauf, dass Transparenz unter den Bedingungen der modernen Informationsverarbeitung nicht einfach als existent angenommen werden kann, sondern explizit erzeugt werden muss, verwies schon früh Steinmüller (1974, S. 201).

[126] Siehe schon dazu Brinckmann et al. (1974, S. 80 f.).

[127] Siehe schon Steinmüller (1975c, S. 144 ff.).

[128] Siehe dazu Podlech (1982, S. 460 f.).

[129] Siehe schon Dammann (1974b, S. 275 ff.) und Podlech (1975b, S. 73), zu den theoretischen Fundamenten der Forderung nach Vorrang der Selbstdarstellung siehe Goffman (1956) und Luhmann (1986). Das gilt, so die Datenschutzkommission des Deutschen Juristentages (1974, S. 26 ff.), auch für öffentliche oder veröffentlichte Informationen, vor allem wenn sie „um einer öffentlichen – vor allem auch politischen – Wirkung willen ganz bewußt in die Öffentlichkeit“ getragen worden seien.

[130] Siehe dazu schon für den öffentlichen Bereich Schlink (1973, S. 159).

[131] Siehe etwa Stalder (2002a, S. 122 f.).

Die zentrale, aus dem Speichern erwachsende Bedrohung liegt gerade in dem, wozu das Speichern dient: ihrer Verfügbarkeit für eine spätere Reproduktion – Aufrufen, Abrufen, Verändern, Übermitteln und Nutzen. Die Verstetigung vormals nur flüchtiger Informationen, die mit dem Akt des Speicherns zugleich beginnen zu veralten, transzendiert die zeitliche Beschränkung von Ereignissen und mithin jede Zeitgebundenheit von Bedeutung, Einordnung und Bewertung dieser Ereignisse, die so nicht nur zur Basis künftiger Entscheidungen werden,[132] sondern zugleich die Möglichkeiten von anderen Akteurinnen verringern, diese Ereignisse, an denen sie beteiligt waren oder nicht, selbst darzustellen, einzuordnen oder zu bewerten, insoweit sie tendenziell mit der durch die Speicherung vermeintlich objektivierten Fremddarstellung, -einordnung oder -bewertung konfrontiert sind.[133] Ein strukturell vergleichbares Problem erzeugt die Entscheidung der Organisation, Informationen gerade nicht zu speichern, mit der mögliche Folge eines Rechtfertigungszwangs für Betroffene für das Fehlen von Informationen.

Das Verändern von Informationen erzeugt eine große Bandbreite an Risiken, angefangen bei direkten Änderungen an den Zweck-, Bedeutungs- und Bezugsdimensionen von Informationen, aber auch am die Bedeutung beeinflussenden Kontext, in den Informationen stehen oder gestellt werden.[134] Informationen werden auch durch Verdaten und Interpretieren, also die Transformationen von Informationen in Daten und umgekehrt, geändert. Mögliche Folgen von Verdatung sind nicht nur Fehlabbildungen, sondern auch Verkürzungen, Dekontextualisierungen, die Erzeugung von Mehrdeutigkeiten und – zentral – die tendenzielle Ersetzung des abgebildeten Objekts und der dieses Objekt immer nur unvollständig, ungenau und sozial aushandlungsbedürftig beschreibenden Informationen durch den vermeintlich objektiven Datenschatten des Objekts.[135] Und wenn und soweit es keine eindeutigen Interpretationsregeln gibt,[136] besteht mit jeder Interpretation von Daten das Risiko von Fehlkontextualisierung, Fehlinterpretation, sowohl hinsichtlich des Zwecks, der Bedeutung wie auch des Bezugs, und in der Folge auch das Risiko der Fehlbewertung. Das Risiko der Kontext- und Bedeutungsänderung steigt auch, wenn Informationen verknüpft – oder verkettet –, integriert oder aggregiert werden, insbesondere wenn das über Organisations- oder Kontextgrenzen hinweg geschieht.[137] Zugleich nimmt für die Informationen damit der Anschein der Objektivität zu, vergleichbar etwa mit dem Steigen des Anscheins von Korrektheit bei zunehmender Genauigkeit, ebenso wie ihre Nutzbarkeit für Bewertungen vergangenen und Vorhersage zukünftigen Verhaltens. Und nicht zuletzt steigert auch das Trennen von Informationen das Risiko der Kontextänderung, vor allem das Risiko des Kontextverlusts, und der Bedeutungsänderung.

Bedrohungen, die durch das Erzeugen von neuen Informationen aus bereits gespeicherten Informationen entstehen, liegen vor allem in der relativen Unerwartbarkeit oder Unvorhersehbar-

[132] Siehe etwa Rule (1973, S. 29).

[133] Siehe etwa Podlech (1976c, S. 315 f.).

[134] Siehe zum Zweckproblem etwa Ruebhausen und Brim (1965, S. 1199), BVerfG (1970, S. 352), Steinmüller (1971c, S. 85) sowie umfassend Hoffmann (1991) und zusammenfassend Pohle (2015b). Siehe zum Problem von Kontext und Bedeutung etwa Miller (1969, S. 1114 ff.), Rüpke (1976, S. 53) oder Podlech (1982, S. 457 ff.). Änderungen in der sigmatischen Dimension – auf welche Akteurin, welchen Sachverhalt, welches Ereignis bezieht sich eine Information – werden, obwohl die wissenschaftliche Debatte insgesamt sehr daten- oder informationszentriert ist, im Grunde nur im Zusammenhang mit Anonymisieren und Deanonymisieren problematisiert, siehe etwa Hoffman und Miller (1973) und Ohm (2010).

[135] Siehe vor allem zu letzterem Westin (1967, S. 163 ff.), Anér (1972, S. 179), Steinmüller (1975c, S. 146) sowie noch Fiedler (1975, S. 80), der warnt, dass unter diesen Bedingungen „die menschliche Lebenswelt nur noch in der Sichtweise einer bestimmten »Verdatung« aufgefaßt“ werden könne.

[136] Siehe dazu Brunnstein (1975, S. 155 f.).

[137] Siehe Müller (1975b).

keit für die Betroffenen, deren Möglichkeiten zu einer auf den Informationsstand der Organisation angemessenen reagierenden Interaktion mit der Organisation dadurch beschränkt werden.[138] So können Organisation etwa auf der Basis von Informationen Kategorien bilden – oder durch technische Systeme bilden lassen: Clustern –, in die die Informationen dann eingeordnet werden, um in der Folge die Einordnung selbst zur Grundlage von Entscheidungen zu machen.[139] Auch die Verwendung unscharfer Suchverfahren erzeugt, vor allem im Vergleich mit einer „einfachen" Suche, besondere Risiken, auch weil – wie auch bei der Verwendung von Heuristiken im Gegensatz zur Verwendung von Algorithmen – nicht sichergestellt werden kann, dass das Sucherergebnis nicht schlicht ein Artefakt ist, dass durch die Fuzziness der Suche erst erzeugt wurde.[140] Und nicht zuletzt entstehen neue Bedrohungen durch die zunehmende Verwendung von korrelationsbasierten Verfahren,[141] vor allem wenn die Ergebnisse solcher Verfahren, nämlich die berechneten Korrelationen, für Kausalitäten gehalten werden.

Neben das schon allgemein beschriebene Risiko einer möglichen Kommunikations-, Entscheidungs- und Handlungsbeeinflussung oder -steuerung der Empfängerinnen von Informationen – etwa auch eines allgemeinen Publikums oder der Öffentlichkeit –, das sich aus der Kontrolle der übermittelnden Organisation über die Weltdarstellung ergeben[142] treten durch eine Übermittlung die Risiken, die sich aus dem faktischen Kontrollverlust der Organisation über die übermittelten Informationen ergeben. Dazu gehören etwa die Risiken für die Vertraulichkeit der Informationen und ihre Kontextualität – und damit ihre Bedeutung –, aber vor allem die Möglichkeiten weiterer – auch zweckfremder – Nutzung und Übermittlung sowie allgemein ihrer Kommodifizierung.[143]

Gerade auch in der Nutzung von Informationen kann sich das schon allgemein beschriebene Datenmachtproblem verwirklichen – die Beeinflussung oder gar Steuerung von individuellen, kollektiven oder institutionellen Betroffenen und ihrer Kommunikationen, Entscheidungen und Handlungen sowie die Prästrukturierung ihrer Handlungsmöglichkeiten. Besondere Risiken ergeben sich für Betroffene bei der Nutzung von Informationen für Zwecke, zu denen sie nicht erhoben wurden,[144] die Nutzung beliebiger – und mit den Betroffenen oder ihrer Situation nichts zu tun zu habender – Informationen zur Entscheidung über Betroffene[145] oder diskriminierende

[138] Siehe schon Steinmüller et al. (1971, S. 87), Müller (1975a, S. 121), aber auch – wenn auch nicht explizit auf erzeugte Informationen bezogen – BVerfG (1983, S. 43).

[139] So zuerst wohl Simitis (1986, S. 29) und Simitis (1987, S. 719, 728), später als „panoptic sort" und „social sorting" von den Surveillance Studies übernommen, siehe Gandy (1993) und Lyon (1994). Zum allgemeinen Problem des „Aussortierens" von Menschen siehe Steinmüller (1971c, S. 82).

[140] Zur Rasterfahndung, bei der es sich um eine Kombination von Verkettung von Informationen und unscharfen Suchen handelt, siehe etwa Enzensberger (1979b) und Herold (1980, S. 82 f.) sowie zum amerikanischen Äquivalent „computer matching" siehe etwa Shattuck (1984).

[141] Eine frühe Problematisierung findet sich bei Lemke (1975, S. 163), allerdings noch unter dem Label „Aggregation". Siehe auch Palley (1986) und Clarke (1988, S. 507) sowie aktuell boyd und Crawford (2011), Pohle (2014b) und Barocas und Selbst (2015).

[142] Siehe etwa Dammann (1976b) und Caplan und boyd (2016). Solche manipulierenden Folgen treten dabei nicht nur unbedingt dann auf, wenn die Übermittlung in manipulativer Absicht geschieht.

[143] Siehe schon Steinmüller (1975c, S. 144) für die Risiken der Kommodifizierung von Informationen über einzelne Akteurinnen sowie humdog (1994) über soziale Beziehungen.

[144] Das folgt schon aus der modelltheoretischen Interpretation des Informationsbegriffs, siehe Podlech (1976d). Das gilt nicht nur dann, wenn die Zwecke von der Organisation explizit der Informationserhebung zugrunde gelegt wurden – Entscheidungsprämissen können gerade auch institutionalisierter Bias als „blind spots in its visual field" sein, so Gandy (1993, S. 16).

[145] Siehe dazu Pohle (2016b).

Entscheidungen.[146] Nicht zuletzt können auch Fehlbewertungen oder Fehlentscheidungen eine Bedrohung darstellen.[147]

Die Risiken, die von einem Sperren und Löschen ausgehen, sind vergleichbar: Fälschlich oder unberechtigt gelöschte oder gesperrte Informationen können zu Nachweisproblemen für Betroffene führen und Fehlbewertungen oder Fehlentscheidungen – oder sogar die Weigerung, ohne diese Informationen eine Entscheidung zu treffen – auslösen, bei gesperrten Informationen gegenüber oder durch alle von der Sperrung betroffenen Organisationsteile und bei gelöschten Informationen gegenüber oder durch die Organisation als Ganzes. Strukturell die gleichen Risiken können durch Pseudonymisieren oder Anonymisieren entstehen.

Die Bedrohungen, die von informationstechnischen Systeme ausgehen oder verstärkt werden, betreffen grundsätzlich alle Akteurinnen, sowohl Betroffene wie Techniknutzerinnen, und darunter wiederum Betroffene, die die Technik nutzen, ebenso wie Mitarbeiterinnen der Organisation, denn die Technik „bestimmt den Spielraum möglichen Verhaltens der Institutionen, Gruppen und Mitglieder der Gesellschaft."[148] So sind grundsätzlich alle Systeme tendenziell intransparent für Nutzerinnen und Betroffene – eine Tendenz, die von der Trennung zwischen (grafischer) Oberfläche und „Innenleben" noch verstärkt wird – und bezieht sich sowohl auf die in die Technik hineinkonstruierte „Politik"[149] als auch die vorhandenen oder nicht vorhandenen Schutzmechanismen und deren Eigenschaften, etwa ihre Qualität. Vor diesem Hintergrund ist es für Betroffene – und wenigstens in Teilen auch für Nutzerinnen – quasi unmöglich, überhaupt eine sinnvolle, weil informierte Risikoabschätzung vorzunehmen und auf dieser Basis über eine Preisgabe und die Bedingungen, unter die diese Preisgabe gestellt werden sollen, zu entscheiden. Auch kann die Organisation Technik nicht wirklich kontrollieren – und damit Eigenschaften wie etwa Diskriminierungsfreiheit nicht garantieren –, die sie selbst zwar einsetzt, aber nicht versteht. Und sie kann nach außen nicht transparent machen, was aus den technischen Systemen heraus nicht expliziert werden kann. Besonders deutlich wird dies bei den inzwischen recht verbreitet eingesetzten neuronalen Netzen. Nutzerinnen innerhalb und außerhalb der Organisation sehen nur, was die Systeme ihnen zeigen, und sie sehen es, wie die Systeme es ihnen zeigen; die informationstechnischen Systemen bestimmen damit das Weltbild der Nutzerinnen mit.[150] Und die Systeme lassen auch Selbstdarstellung von Nutzerinnen nur insoweit zu, wie es ihnen eingebaut wurde.[151] Das gilt auch gegenüber Organisationen, die informationstechnische Systeme

[146] Siehe umfassend Zarsky (2014). Entscheidungen diskriminieren immer, denn sie sind – wie alle Informationen – Unterschiede, also Unterscheidungen, die einen Unterschied machen, siehe Bateson (1987, S. 321). Zu fragen ist hier also, *was* als Unterscheidungskriterium genutzt wird und ob das für die Betroffenen und die Gesellschaft akzeptabel ist oder nicht.

[147] Siehe auch hier der Hinweis bei Steinmüller (1975a, S. 521, Fn. 36), dass immer geprüft werden müsse, ob „»richtige« oder »falsche« [Entscheidungen] »nützlicher« oder »gefährlicher« für Interessenten und Betroffene sind."

[148] Podlech (1988, S. 118).

[149] Siehe schon Winner (1980).

[150] Für Computer als Medien gilt dann Luhmanns Ausspruch über die Massenmedien: „Was wir über unsere Gesellschaft, ja über die Welt, in der wir leben, wissen, wissen wir durch die Massenmedien", Luhmann (1995, S. 9).

[151] Siehe Pohle (2016c, S. 12), Hervorhebung im Original: „Wer sich nur entscheiden kann, sich selbst in einem Formular als »männlich« oder als »weiblich« zu bezeichnen, kann sich eben auch nur *innerhalb dieser Vorgaben* frei entscheiden. Und während ein papiernes Formular noch die Möglichkeit zur praktischen Dissidenz bietet und es erlaubt, an dieser Stelle »ich« einzutragen, kann in computerisierten Systemen eine solche Möglichkeit wirksam unterbunden werden – zwei gekoppelte Radiobuttons, die eine Entscheidung erzwingen, weil sich das System andernfalls weigert fortzufahren, genügen. Damit lassen sich individuelle und gesellschaftliche Alternativlosigkeiten erzeugen, die als objektiv erscheinen."

einsetzen: Betroffene verlieren Interventions- und Aushandlungsmöglichkeiten, wenn diese Systeme solche Möglichkeiten nicht zulassen.[152] Kurz: Informationstechnische Systeme sind nicht nur „Machtverstärker“,[153] sondern, weil sie geronnene Organisation sind, auch Problemverstärker.

Ein für die Gestaltung von informationstechnischen Systemen nutzbares Bedrohungsmodell muss auf der Basis dieses analytischen Rasters das Problem der Machtverschiebung zwischen den Akteurinnen durch das zu gestaltende oder einzusetzende Verfahren sowie die sich aus den einzelnen Verfahrenskomponenten in den einzelnen Verarbeitungsphasen ergebenden genauso wie die komponenten- und phasenübergreifenden besonderen Risiken und Bedrohungen anwendungsbereichsspezifisch konkretisieren.

3.5.3 Operationalisierungs- und Regelungsansatz

Eine allgemeine „Lösung“ des Datenschutzproblems kann es ebenso wenig geben wie ein allgemeines und dennoch immer passgenaues Bedrohungsmodell. Nachfolgend soll daher ein prozeduraler Operationalisierungsansatz vorgelegt werden, der zumindest den Lösungsweg hinreichend deutlich beschreibt und der zugleich für eine rechtliche Regelung wie für Technikgestaltungsprozesse nutzbar ist, dabei auftretende Probleme – so das Checklisten-Problem – anspricht und zeigt, wie mit Hilfe eines der Zwischenprodukte der Analyse – der Interessen-, Zweck- und Machtanalyse – das in der Debatte der letzten Jahrzehnte als besonders drängend markierte Problem der informierten Einwilligung grundsätzlich lösbar gemacht werden kann. Gerade vor dem Hintergrund, dass konkrete Bedrohungen nur anhand konkreter Informationssystemen identifiziert und auch nur in diesen gelöst werden können, erscheint ein solcher prozeduraler Ansatz vorzugswürdig.[154]

Die Prozeduralisierung erzeugt tendenziell das Checklisten-Problem: Das Ausfüllen der Checkliste wird zum Ersatz für eine inhaltliche Auseinandersetzung aufseiten der Ausfüllenden, die ausgefüllte Checkliste wird zum eigentlichen Ziel der Analyse und zum Erfolgsmarker für eine Datenschutzaufsicht, die im Zweifel selbst auch nur Checklisten ausfüllt. Die Frage, die sich also stellt, lautet: Wie kann ein Prozess gestaltet werden, der die einzelnen abzuarbeitenden Analyseschritte grundsätzlich nur in eine Reihenfolge bringt und bei der Sicherstellung einer vollständigen Abdeckung aller Schritte hilft, um eine sinnvolle – also fundierte inhaltliche (oder materielle) – Prüfung innerhalb der einzelnen Schritte zu erzwingen? Insbesondere muss verhindert werden, dass diejenigen, die eine solche Analyse durchführen, eine inhaltliche Prüfung mittels Phrasen wie „Überwiegende berechtigte Interessen der Betroffenen sind nicht ersichtlich.“ als „Prüfungsergebnis“ simulieren können. Wie also kann der Prozess so gestaltet werden, dass anhand der Produkte des Prozesses überprüfbar wird, dass eine fundierte inhaltliche Prüfung stattgefunden hat?[155] Die beiden Fragen können hier nicht allgemein beantwortet werden, aber es lässt sich zumindest die plausible Hypothese aufstellen, dass eine Transparenzpflicht für die Zwischenprodukte – das sind nachfolgend die Anwendungsbereichsbestimmung, die Akteursanalyse sowie die Interessen-, Zweck- und Machtanalyse – die Überprüfbarkeit des Bedrohungsmodells zumindest stark erleichtern würde. Das gilt vor allem, wenn erstens die Zwischenprodukte hinreichend

[152] Siehe etwa Podlech (1982, S. 460).

[153] Steinmüller (1993, S. 417).

[154] Nicht nur entspricht ein solches Vorgehen dem historisch zugrunde gelegten Verständnis einer Anbindung des Datenschutzes an die Verfahrensgestaltung, siehe Pohle (2014b, S. 91 ff., Rn. 13 ff.), sondern es ist auch besser anschlussfähig an die Vorstellungen der operativen Systemtheorie, siehe Luhmann (2000, S. 146), sowie die informatischen Vorstellungen von „Vorgehensmodellen“ im Bereich der Systementwicklung, siehe etwa das Vorgehen bei Notario et al. (2015). Zur Kritik an der Prozeduralisierung des Datenschutzes im Recht siehe aber De Hert und Gutwirth (2006, S. 87 ff.).

[155] Die gleiche Frage könnte im Hinblick auf das verfassungsrechtliche Zitiergebot gestellt werden.

standardisiert werden, um vergleichbar zu sein, ohne zugleich übermäßig formalisiert zu werden und damit selbst als Checklisten-Äquivalente zu enden, und wenn sie zweitens standardisiert verfügbar sind, vergleichbar etwa der `robots.txt` oder den P3P-Versuchen der Vergangenheit. Nicht nur können sie dadurch verglichen werden, sie können vor allem industrialisiert verglichen werden – in einem ersten Schritt zu einer Industrialisierung des Datenschutzes.

Zugleich können die Produkte der Akteursanalyse sowie der Interessen-, Zweck- und Machtanalyse für eine pragmatische Lösung des Problems der informierten Einwilligung genutzt werden. Die von den Organisationen – oder zumindest aus Organisationssicht – erzeugte Beschreibung der Akteurinnen in Form einer Selbstbeschreibung der Organisation und einer Fremdbeschreibung aller Betroffenen(-gruppen),[156] die ihnen zugeschriebenen Rollen und gesellschaftlich geprägten Erwartungen, die ihnen zugeschriebenen Interessen, Rechte, Pflichten, Ziele und Zwecke, und die Beschreibung des Verhältnisses, insbesondere des Machtverhältnisses, in dem die Akteurinnen als zueinander stehend angenommen werden, können von Betroffenen als Grundlage für die Entscheidung genommen werden, ob sie die Selbstzuschreibung der Organisation für vertrauenswürdig, die auf sie selbst bezogene Fremdzuschreibung für fair und die Darstellung der Interessengegensätze, Zweckkollisionen und Machtverhältnisse für angemessen hält – und damit als Basis für die Entscheidung, ob sie in eine sie betreffende Verarbeitung von Informationen einwilligen oder nicht. Mit einem an das Zweckbindungsprinzip angelehnte Modellbindungsprinzip kann dann zugleich sichergestellt werden, dass die auf dieser Basis durchgeführte anwendungsbereichsspezifische Bedrohungsanalyse nicht von der Organisation beliebig manipuliert werden kann, weil wesentliche Teile anhand der zugrunde gelegten Modelle für Dritte wie Aufsichtsorgane, Prüfinstitutionen oder Datenschutzvereinigungen objektiv überprüfbar gemacht werden.

In einem ersten Schritt ist damit der Anwendungsbereich des zu gestaltenden oder des zu prüfenden Verfahrens oder – im Rahmen von Technikgestaltung oder Technikprüfung – des informationstechnischen Systems festzulegen oder zu bestimmen.

Im zweiten Schritt sind die beteiligten oder zu beteiligenden Akteurinnen zu identifizieren und zu beschreiben.[157] Dazu zählen nicht nur die Organisation, ihre Mitarbeiterinnen, die Verdaten und eventuelle Dritte, etwa Empfängerinnen, sondern gerade auch relevante Teilgruppen, die aber durchaus typisiert werden können: In Bezug auf die Mitarbeiterinnen sind etwa Admins und einfache Userinnen klassische Typen, in Bezug auf die Betroffenen lassen sich Gruppen nach den unterschiedlichen Risiken in unterschiedlichem Umfang bilden, denen sie ausgesetzt sind, während Dritte sich unterteilen lassen nach Individuen oder der Öffentlichkeit, den klassischen Angreifertypen oder der NSA, Gruppen oder Organisationen, Akteurinnen mit ökonomischen oder mit politischen Interessen. Für diese Akteurinnen ist dabei zu identifizieren, in welchen Rollen sie auftreten. Damit sind nicht nur die gesellschaftlich konstruierten Rollen wie Individuum, Subjekt, Familienmitglied, Bürgerin, Kundin, Patientin oder Mandantin für Menschen – als Personenkonzepte[158] – oder Behörde, Unternehmen oder Presse für Organisationen gemeint, sondern auch die konkreten Handlungsrollen wie Technikgestalterin, Admin, Anbieterin, Nutzerin, Freundin oder Studentin, in denen sie jeweils miteinander und mit der Technik interagieren. Anhand dieser Rollen lassen sich dann schon die gesellschaftlich geprägten Erwartungen und die gesellschaftlich konsentierten Interessen identifizieren und zuweisen, also die

[156] Siehe dazu umfassend Kieserling (2004).

[157] Dabei ist unschädlich, dass es sich nur um Zuschreibungen handelt, denn erstens liefert auch eine Angreiferanalyse in der IT-Sicherheit nichts anderes – es wäre eher überraschend, wenn ein Angreifermodell auf einer Selbstbeschreibung der Angreiferinnen basierte – und zweitens dient gerade die Zuschreibung *durch die Organisation* als Basis für ihre Bewertung durch die Betroffenen auf Vertrauenswürdigkeit und Fairness.

[158] Siehe dazu und zum Verhältnis zum Datenschutz Rost (2013b).

Freiheits- und Partizipationsversprechen der modernen bürgerlichen Gesellschaft[159] und sogar ihre Strukturschutzprinzipien und -mechanismen, aber durchaus auch individuelle oder kollektive Erwartungen und Interessen der jeweiligen Akteurinnen.[160] Anschließend sind die Zwecke zu identifizieren, die die Akteurinnen jeweils verfolgen. Das können politische oder ökonomische Zwecke sein, aber auch zwischenmenschliche Kommunikation wie Small Talk. Klar ist, dass die unterschiedlichen Akteurinnen jeweils nicht die gleichen Interessen haben oder die gleichen Zwecke verfolgen müssen, trotzdem können sie miteinander interagieren.

Im dritten Schritt sind daher die Interessen und Zwecke vor dem Hintergrund, in welchem Verhältnis die Akteurinnen zueinander stehen, vor allem in welchem Machtverhältnis, und inwieweit sie voneinander abhängig sind, etwa von der Erbringung einer spezifischen Leistung wie der Bereitstellung einer Kommunikationsinfrastruktur für die Kommunikation mit anderen, zueinander in Beziehung zu setzen und zu analysieren.[161] In dieser Interessen-, Zweck- und Machtanalyse muss deutlich werden, inwieweit die Interessen und Zwecke der unterschiedlichen Akteurinnen einander entsprechen, kompatibel sind oder einander widersprechen, welche Interessen und Zwecke nur durchgesetzt oder erreicht werden können, wenn andere Akteurinnen kooperieren, und von welchen Akteurinnen Kooperation zu erwarten ist und von welchen nicht. Darüber hinaus ist zu analysieren, welche Folgen sich für die Machtbeziehungen zwischen den Akteurinnen ergeben oder ergeben können, wenn Akteurinnen ihre Interessen und Zwecke auch gegen die Interessen und Zwecke anderer Akteurinnen durchzusetzen in der Lage sind. Anschließend sind diese Interessen und Zwecke zu gewichten und zu bewerten, um darauf basierend zwischen den widerstreitenden Interessen und Zwecken abzuwägen. Datenschutz steht dabei konsequent aufseiten der strukturell schwächeren Akteurinnen und schreibt sich die Durchsetzung ihrer Interessen gegen die Interessen der ungleich mächtigeren Organisationen auf die Fahne, und in diesem Sinne sind auch Gewichtung, Bewertung und Abwägung vorzunehmen.[162] Die eigentliche Zwecksetzung für das Informationssystem ist eines der Ergebnisse dieses dritten Schritts.[163]

[159] Selbst in einer juristischen Analyse sollte an dieser Stelle noch keine Beschränkung auf bestimmte Rechte vorgenommen werden, etwa auf Grundrechte oder grundrechtsgleiche Rechte, da sich der Analyserahmen damit zu früh verengen würde. Die Frage, welche Qualität oder welches Gewicht die Interessen haben, sollte erst beantwortet werden, wenn die Interessen der verschiedenen Akteurinnen zusammengetragen und einander gegenübergestellt worden sind.

[160] Siehe dazu etwa den Stakeholder-Ansatz, Freeman (2004).

[161] Siehe dazu schon Podlech (1983, S. 213 ff.) sowie mit dem Ziel eines Surveillance Impact Assessments Wright und Raab (2012).

[162] Das erklärt sich auch aus der Identifikation der Schutzgüter des Datenschutzes: Freiheits- und Partizipationsversprechen auf der einen und Strukturschutzprinzipien und -mechanismen auf der anderen Seite. Im bürgerlichen Verfassungsverständnis dienten Grundrechte als besonders herausgehobene Verkörperungen dieser Freiheits- und Partizipationsversprechen schon immer dem Schutz der Schwachen – der Menschen, der Bürgerinnen, der Privaten – und der Abwehr von Übergriffen des Starken – des Staates. Daran ändert sich strukturell auch nichts, wenn die Geltung von Grundrechten auch auf das Verhältnis zwischen Privaten ausgedehnt wird. Insofern stellt es im Grunde eine Perversion der Idee von Grundrechten dar, wenn stärkere Akteurinnen Grundrechtsschutz gegen schwächere verlangen und bekommen. Und auch die verfassungsrechtlich normierten Strukturschutzprinzipien und -mechanismen dienen der Machtbeschränkung der Starken, nicht dem Ausschluss der Schwachen.

[163] Mit der Verlegung der Entscheidung über den Zweck ans Ende der Interessen-, Zweck- und Machtanalyse erhöht sich der Rechtfertigungsdruck für einseitige, den Interessen und Zwecken der Betroffenen entgegengerichtete Zwecksetzungen durch die Organisationen. Damit wird also die Zwecksetzung selbst zum diskutierbaren Teil der das System definierenden Vorentscheidungen der Organisation und erhöht damit die Chance, dass Betroffene informierte Entscheidungen darüber treffen können, ob sie mit der betreffenden Organisation informationell interagieren wollen oder nicht, und zu welchen Bedingungen. Zugleich wird damit für Organisationen das Problem der Zweckspezifizierung, also die Frage, wie abstrakt oder konkret, wie weit oder eng der Zweck festzulegen ist, lösbar. Die Entscheidungsheuristik würde dann lauten: Je divergenter die Interessen und Zwecke

Die anwendungsbereichsspezifische Bedrohungsanalyse stellt den vierten Schritt dar und dient der Erzeugung des oben beschriebenen Bedrohungsmodells.

Der fünfte Schritt ist dann die Auswahl und Gestaltung von Lösungen für die identifizierten Bedrohungen auf der Basis von materiellen Anforderungen. Diese materiellen Anforderungen sind sachlich in Form von Schutzzielen zu formulieren,[164] die dazu nicht wie bislang aus dem geltenden Datenschutzrecht, sondern direkt aus der Datenschutztheorie abgeleitet werden müssen. Diese Schutzziele sind dabei so zu formulieren, dass sie sich nicht nur auf Verfahren mit den Komponenten Informationen, Prozesse und Systeme anwenden lassen, sondern auch auf die Organisationen selbst und deren Gestaltung.[165] In zeitlicher Hinsicht sind diese Anforderungen phasenspezifisch zu konditionieren, aber wegen der Eigenschaften komplexer Systeme,[166] zu denen inzwischen wohl die meisten automationsgestützten Verfahren gehören, sind sie nicht auf die Phasen zu beschränken.[167] Und in sozialer Hinsicht ist – angelehnt an das Prinzip der Gewaltenteilung – dafür zu sorgen, dass die Kontrolle über bestimmte Verfahrensaspekte nicht nur innerhalb von Organisationen, sondern auch zwischen Organisationen und Betroffenen verteilt sind – und das nicht nur organisatorisch, sondern auch technisch.[168]

Dieser Operationalisierungs- und Regelungsansatz, der hier in einer noch sehr rohen oder abstrakten Form vorgelegt wird, muss in der Praxis verwendet und damit getestet und auf der Basis der dabei gewonnenen Erkenntnisse überarbeitet und konkretisiert werden. Dazu gehören insbesondere auch die Ableitung der Schutzziele aus der Datenschutztheorie sowie ihre phasenspezifische Konditionierung.

3.6 Das Recht des Datenschutzes

Das Recht, das versucht, die vom hier dargestellten und rekonzeptionalisierten Datenschutz adressierten individuellen und gesellschaftlichen Probleme zu lösen, lässt sich nicht nur in dem Rechtsbereich verorten, der explizit als Datenschutzrecht bezeichnet wird. Dieser Bereich umfasst die einschlägigen Grundrechte, vor allem das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts, das BDSG zur Regelung des Umgangs mit personenbezogenen Informationen durch private Stellen sowie öffentliche Stellen des Bundes, die Landesdatenschutzgesetze für öffentliche Stellen der Länder und die bereichsspezifischen Datenschutzregelungen in einzelnen Fachgesetzen, aber auch die neue EU-DSGVO. Rechtliche Regelungen zum Datenschutz im hier verstandenen Sinne finden sich aber eben auch in vielen anderen Gesetzen, die informationell begründete oder verstärkte Machtpositionen adressieren.

sind, desto konkreter muss der Zweck spezifiziert werden. Je asymmetrischer das Machtverhältnis ist, desto enger muss der Zweck gesetzt werden.

[164] Siehe grundlegend Rost und Pfitzmann (2009) sowie Bock und Rost (2011), Rost (2012b), Rost und Storf (2013) und Hansen et al. (2015).

[165] Dabei geht es weder um die Gleichsetzung von Organisation und Maschine im Weberschen Sinne noch im Sinne der Kybernetik. Aber wie Rost und Storf (2013) für die Verwendbarkeit von Schutzzielen für die „Vermittlung“ zwischen Recht und Technik zeigen, lässt sich plausibel vermuten, dass Schutzziele auch zwischen Technik und Organisation vermitteln können.

[166] Siehe Simon (1962, S. 468): „In such systems, the whole is more than the sum of the parts, not in an ultimate, metaphysical sense, but in the important pragmatic sense that, given the properties of the parts and the laws of their interaction, it is not a trivial matter to infer the properties of the whole.“

[167] Siehe auch Pohle (2016c, S. 9).

[168] Diese drei Dimensionen – sachlich, zeitlich, sozial – entsprechen den drei Sinndimensionen bei Luhman, siehe grundlegend Luhmann (1964a, S. 59 f.) und Luhmann (1987, S. 112). Ich danke Martin Rost für diesen Hinweis und die Diskussion, deren Ergebnis dieses Strukturkonzept für materielle Datenschutzanforderungen ist.

Dazu gehören etwa die Informationsfreiheitsgesetze des Bundes und der Länder sowie die Transparenzregelungen verschiedener Fachgesetze, parlamentarische Auskunfts- und Untersuchungsrechte, die Monopolverhinderungs- oder -beschränkungsregelungen im Medien- und Telekommunikationsbereich aber auch das Verbot aggressiver geschäftlicher Handlungen nach § 4a UWG, etwa durch eine „die Fähigkeit des Verbrauchers oder sonstigen Marktteilnehmers zu einer informierten Entscheidung wesentlich einschränk[enden]“ Technikgestaltung unter Ausnutzung einer „Machtposition gegenüber dem Verbraucher oder sonstigen Marktteilnehmer“. Eine umfassende Darstellung dieses gesamten *Rechts des Datenschutzes* würde den Rahmen der vorliegenden Arbeit sprengen und muss daher an anderer Stelle geschehen.[169] Das gilt selbst für eine umfassende Darstellung des Verhältnisses zwischen Datenschutz und Datenschutzrecht.[170]

Nachfolgend soll daher in aller gebotenen Kürze das für die Technikgestaltung relevante Verhältnis zwischen dem hier beschriebenen Datenschutz und dem geltenden Datenschutzrecht, das historisch wesentlich von der hier betrachteten Datenschutztheorie und ihren Vertreterinnen geprägt wurde und – wenn auch inzwischen weniger – bis heute beeinflusst ist, bestimmt werden, vor allem im Hinblick auf den Geltungsbereich, den verwendeten Informationsbegriff und den Umgang des Rechts mit dem Prozessmodell der Informationsverarbeitung.

Das Datenschutzrecht setzt diese Modelle nicht einfach nur um. Zwar ist es historisch stark von ihnen geprägt, zugleich ist es aber das Produkt politischer Aushandlungen in Parlamenten, beeinflusst von den verschiedenen Stakeholdern in Gesetzgebungsverfahren sowie ausgelegt und reinterpretiert in juristischen Fachdiskussionen und von Gerichten. Das Datenschutzrecht bestimmt seinen eigenen Geltungsbereich, seine eigenen Schutzgüter und seine eigenen Mechanismen, die jeweils nicht denen entsprechen müssen, die die Datenschutztheorie produziert hat. Die Datenschutztheorie und ihre Modelle können zur Auslegung des Rechts verwendet werden, sie können aber gleichwohl die Ketten des Rechts nicht sprengen, denn der Befolgungsanspruch des Datenschutzrechts endet an den Grenzen seines Geltungsbereiches. Wo das bestehende Datenschutzrecht keinen hinreichenden Schutz für die Betroffenen vor den von der Datenschutztheorie identifizierten Bedrohungen gewährleisten kann oder will – und auch andere Gesetze nicht einschlägig sind –, liegt der Bereich der freien Entscheidung der Gestalterinnen der Technik, die Anforderungen des Datenschutzes trotzdem umzusetzen. Und von dieser Freiheit sollten sie Gebrauch machen.

3.6.1 Geltungsbereich

Die Geltungsbereiche von Datenschutz und Datenschutzrecht überschneiden sich, sind jedoch weder deckungsgleich, noch ist eines eine Teilmenge des je anderen. Der Schutzbereich des Datenschutzrechts ist signifikant kleiner als der des Datenschutzes, zugleich ist der Kreis der Normadressatinnen des Datenschutzrechts signifikant größer.

Der wesentliche Grund für den gegenüber dem Datenschutz – und selbst dem Individualdatenschutz im Verständnis des 1971er Gutachtens – signifikant verkleinerten Schutzbereich des Datenschutzrechts liegt in der Nutzung des Konzepts der „personenbezogenen Daten“ als

[169] Ein erster Schritt dazu liegt mit der „Matrix des Datenschutzes“, siehe von Lewinski (2014), bereits vor, wenn auch nur insofern umfassend, als dass die Arbeit einen Überblick über alles gibt, was in der Debatte irgendwie als „Datenschutz“ markiert wurde oder wird, und dabei zugleich eine deutliche Schlagseite zugunsten individueller und zuungunsten gesellschaftlicher Problembereiche aufweist.

[170] Für den zu erwartenden Aufwand für eine solche Darstellung siehe Woertges auf den Individualdatenschutz beschränkte Dissertation „Die Prinzipien des Datenschutzrechts und ihre Realisierung im geltenden Recht“, Woertge (1984).

Abgrenzungskriterium, die zugleich aber konsistent ist mit grundsätzlich allen im vorherigen Kapitel betrachteten *information-privacy*-Theorien.[171] Nach § 3 Abs. 1 BDSG sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person", die zugleich als „Betroffener" definiert wird, während Art. 4 Nr. 1 EU-DSGVO sie definiert als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen" und dabei eine Person „als identifizierbar [ansieht], die [...] identifiziert werden kann". Der Begriff „identifizieren" wird in der juristischen Auseinandersetzung an keiner Stelle problematisiert, verweist aber deutlich auf die impliziten Vorannahmen über den Charakter der Informationsverarbeitung: Alle diese Beschreibungen gehen davon aus, dass es zu einem bestimmten Zeitpunkt t nur die Informationen gibt, zu der dann die Person „gefunden" werden soll, auf die sich diese Informationen beziehen.[172] Das Problem der Adressierbarkeit, das für Kommunikationen typisch ist, bleibt in der ganzen Debatte ausgeblendet.[173] Während damit das Element der Bestimmbarkeit und Identifizierbarkeit zu einer signifikanten Beschränkung der Menge der Betroffenen führt,[174] wird das Beziehungselement durchgängig weit verstanden.[175] Die Gruppe der Betroffenen ist aber nicht nur hinsichtlich der Identifizierbarkeit beschränkt, sondern vor allem dahingehend, dass als Betroffene im deutschen und europäischen Datenschutzrecht nur natürliche Personen gefasst werden.[176] Damit dient das Datenschutzrecht weder dem Schutz von Gruppen,[177] der allerdings inzwischen wieder gefordert wird,[178] noch dem Schutz von anderen sozialen Akteurinnen wie Organisationen, ob als Personengesellschaften oder juristische Personen.[179]

[171] Das Konzept der personenbezogenen Informationen ist dabei sowohl in der Theorie wie auch im Recht – weltweit – zum Fixpunkt der Auseinandersetzung geworden, dass sich durchaus von einer „Fixierung" sprechen lässt, so kritisch Pohle (2016b).

[172] Das ist im Grunde des Unterstellung einer aktenführenden Bürokratie, die nach Aktenlage entscheidet und dabei Entscheidungen über Menschen nur auf der Basis von Informationen über diese Menschen trifft, Pohle (2016b, S. 16). Und dafür ist es notwendig, diese Menschen „genau wieder[zu]erkennen" oder ihre „Identität [...] fest[zu]stellen", so der Duden zu den einschlägigen Bedeutungen von „identifizieren", siehe `http://www.duden.de/suchen/dudenonline/identifizieren`, abgerufen am 20.06.2016. Anders nur Rihaczek, der „personenbezogene (auf die natürliche Person des Bürgers bezogene) Interessen an Daten", und „nicht nur [...] Interessen an »personenbezogenen Daten«" zum Anknüpfungspunkt des Rechts machen will, siehe Rihaczek (1980, S. 229). Selbst die scheinbar ähnliche Forderung der Article 29 Data Protection Working Party (2007, S. 10 f.) zu den Zweck- und Ergebniselementen von Informationen bezieht sich nur auf den „relating to"-Teil der Definition – „any information relating to an identified or identifiable natural person" –, nicht aber auf den „identified or identifiable"-Teil.

[173] Siehe selbst die Darstellung am Ende von Rn. 10 bei Simitis (Dammann in: 2011, § 3) sowie Rn. 63, Däubler et al. (Weichert in: 2010, § 3, Rn. 14) sowie Erwägungsgrund 30 der EU-DSGVO – immer geht es nur um gespeicherte Informationen, für die zu einem späteren Zeitpunkt ein Personenbezug hergestellt werden soll, aber nicht um die Nutzbarkeit für Entscheidungen innerhalb der Transaktionen oder Sitzungen.

[174] Siehe dazu auch schon die Ausführungen zu Transaktionen und Anonymität im vorherigen Kapitel. Damit erklärt sich auch, warum etwa Däubler et al. (Weichert in: 2010, § 3, Rn. 13) seine Ausführungen zur Bestimmbarkeit damit einleitet, dass diese weit auszulegen sei: Sie ist *außerhalb von Transaktionen* weit auszulegen.

[175] So Simitis (Dammann in: 2011, § 3, Rn. 7), der die Fußnote zur Aussage, dass das sigmatische Element „außerordentlich weit" zu verstehen sei, einleitet mit „[s]tatt aller", siehe Fn. 30.

[176] Siehe § 3 Abs. 1 BDSG zur Betroffenendefinition sowie die Zweckbestimmung des Gesetzes in § 1 Abs. 1 BDSG, die sich nur auf „den einzelnen" bezieht, und Art. 4 Nr. 1 EU-DSGVO für die Definition der „betroffene[n] Person" sowie die Bestimmung des Gesetzeszwecks in Art. 1 Abs. 1 EU-DSGVO.

[177] Es sei denn, insoweit „die zu einer Personenmehrheit gespeicherten Daten zugleich etwas über die Verhältnisse der einzelnen Mitglieder aussagen", Simitis (Dammann in: 2011, § 3, Rn. 19).

[178] Siehe etwa jüngst Mantelero (2016).

[179] So unterfallen etwa in Österreich auch juristische Personen dem Anwendungsbereich des Bundesgesetzes über den Schutz personenbezogener Daten, siehe § 4 Nr. 3. Siehe auch Simitis (Dammann in: 2011, § 3, Rn. 18) für weitere Beispiele. Die dort vorgelegte Begründung gegen einen Schutz von juristischen Personen überzeugt

Während also der Kreis der Betroffenen im Datenschutzrecht kleiner ist als im Datenschutz, ist der Kreis der Normadressatinnen signifikant größer und beschränkt sich dabei nicht nur auf solche, mit denen die Betroffenen in sozialen Beziehungen stehen, die von strukturellen Datenmachtimbalancen geprägt sind. Normadressatinnen des BDSG sind alle – hinsichtlich ihres informationellen Handelns der Regelungskompetenz des Bundes unterfallende – sozialen Akteurinnen, „es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten."[180] Ebenso weit ist der Kreis der Normadressatinnen der EU-DSGVO, wonach die Grundverordnung nur für „natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" keine Anwendung findet.[181] Diese Einschränkungen sind jedoch, spätestens nach der Lindquist-Entscheidung des EuGH,[182] sehr restriktiv auszulegen: Das Gericht übersetzt „persönliche oder familiäre Tätigkeiten" als „Tätigkeiten [...], die zum Privat- oder Familienleben von Einzelpersonen gehören" und erklärt, es handele sich „offensichtlich" nicht um solche Tätigkeiten „bei der Verarbeitung personenbezogener Daten, die in deren Veröffentlichung im Internet besteht, so dass diese Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden."[183] Das ist nicht nur deshalb extrem dysfunktional, weil es soziale Beziehungen, in denen das informationelle Verhalten der Beteiligten tatsächlich noch hinreichend sozial ausgehandelt werden kann, einem bürokratischen Regelungsregime unterwirft, das in seiner Architektur und dem Umfang und dem Formalismus seiner Anforderungen darauf zugeschnitten war, bürokratische Verwaltungen in Staat und Gesellschaft an die Ketten des Rechtsstaatsprinzips zu legen.[184] Das ist zugleich strategisch riskant – und vielleicht deswegen gerade von manchen Beteiligten erwünscht –, weil es große Akteurinnen geradezu einlädt, kleine Akteurinnen als mit der vollen Wucht des Gesetzes Getroffene vorzuschicken, um darüber eine Absenkung der Schutzstandards zu propagieren.[185]

Nicht nur hinsichtlich des Betroffenenkreises und der Fixierung auf personenbezogene Daten, sondern auch im Hinblick auf das Schutzgut ist der Schutzbereich des Datenschutzrechts kleiner als der des Datenschutzes. Zwar mag es ein „Allgemeinplatz" sein, dass es letztlich „um den

aber nicht, gerade auch vor dem Hintergrund, dass die informationelle Selbstbestimmung, auf die dort zentral Bezug genommen wird, ein Plagiat der *privacy*-Konzeption Westins ist, die sich deutlich auf „individuals, groups, or institutions" bezieht, siehe Westin (1967, S. 7).

[180] Siehe § 1 Abs. 2 Nr. 3 BDSG. Dies ist ein bedeutend größerer Adressatinnenkreis als noch der des BDSG 1977, der nur auf solche soziale Akteurinnen abzielte, die „geschützte personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele verarbeiten", § 22 Abs. 1 Satz 1.

[181] Siehe Art. 2 Abs. 2 c) EU-DSGVO.

[182] Urteil des Europäischen Gerichtshofes vom 6. November 2003 in der Rechtssache C-101/01.

[183] Siehe EuGH C-101/01, Rn. 2 und 47. Simitis (Dammann in: 2011, § 1, Rn. 151) fasst darunter etwa alle soziale Netzwerke. Siehe aber auch Erwägungsgrund 18 der EU-DSGVO: „Als persönliche oder familiäre Tätigkeiten könnte auch [...] die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten." Dabei ist aber zu beachten, dass aus Erwägungsgründen keine Rechtsfolgen abgeleitet werden können, sie können nur zur Auslegung herangezogen werden.

[184] Siehe Steinmüller (1976c, S. 14), der das Datenschutzrecht als die „folgerichtige Weiterentwicklung des rechtsstaatlichen Prinzips der Gesetzmäßigkeit der Verwaltung" durch dessen Ausdehnung auf den privaten Bereich bezeichnet und damit zurecht zugleich auf den besonderen Charakter des Datenschutzrechts verweist: Die gesetzlichen Anforderungen sind durchgängig so gehalten, dass sie im Kern voraussetzen, dass die Normadressatin tatsächlich eine rationale Organisation ist, die mit dieser Art von Anforderungen angemessen umgehen kann, ganz zu schweigen von ihrem Umfang.

[185] Für ein solches Beispiel siehe etwa Giesen (2013), der sich zwar an den datenschutzrechtlichen Grundprinzipien, wie dem Verbot mit Erlaubnisvorbehalt abarbeitet, aber fast ausschließlich Individuen als Informationsverarbeiterinnen betrachtet und sich noch dazu wesentlich auf interpersonale, also gemeinschaftliche Beziehungen beschränkt.

Schutz von Menschen“ gehe, „nicht um den Schutz von Daten“,[186] gleichwohl wird in der EU-DSGVO in Art. 1 Abs. 2 – wie vorher auch schon in der EG-DSRL – neben den „Grundrechte[n] und Grundfreiheiten“ sowie fast wortgleich auch in Art. 8 Abs. 1 der EU-Grundrechtecharta das „Recht auf Schutz personenbezogener Daten“ als Schutzgut markiert.[187] Während die durchaus weite Formulierung „Grundrechte und Grundfreiheiten“ als „Rechte und Freiheiten der Betroffenen“ aus der EG-DSRL in § 4d Abs. 5 Satz 1 BDSG übernommen wurde,[188] definiert § 1 Abs. 1 BDSG den Zweck des Gesetzes als Schutz des „Einzelnen“ vor Beeinträchtigung „in seinem Persönlichkeitsrecht“. Auf dieses Persönlichkeitsrecht rekurriert auch das BVerfG im Volkszählungsurteil und stellt fest, dass die „[f]reie Entfaltung der Persönlichkeit [...] unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus[setzt]“ und dieser Schutz „daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt“ sei.[189] Das „Recht auf informationelle Selbstbestimmung“, dem das BVerfG dann als Ausprägung dieses Persönlichkeitsrechts verfassungsrechtliche Weihen verleiht,[190] ist schon eine – doppelte – Verkürzung dieses Schutzes, denn es bezeichnet nur noch „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“[191] Erstens handelt es sich um einen individualistischen Problemlösungsansatz für ein gesellschaftliches Problem, dessen praktische Um- und Durchsetzung die realen Fähigkeiten des Individuums weit übersteigt, und zweitens schützt das Grundrecht gerade nicht gegen eine „unbegrenzte“ Verdatung, solange nur „der Einzelne“ einwilligt.[192] Gleichwohl wird gerade dieses individuelle Verfügungsrecht inzwischen verbreitet als das eigentlich zentrale Schutzgut des Datenschutzrechts betrachtet,[193] auch wenn die genaue verfassungsrechtliche Anknüpfung wenigstens nicht

[186] So von Lewinski (2014, S. 4).

[187] Dass es sich dabei keineswegs um einen sprachlichen Unfall handelt, sondern um die sprachliche Ausprägung eines Verständnisses vom Schutzgut, zeigt sich in einem Vergleich mit sprachlich gleich konstruierten Begriffen wie „Hochwasserschutz“ oder „Sonnenschutz“: Es käme wohl niemand auf die Idee, diese Begriffe in der Form „Schutz des Hochwassers“ oder „Schutz der Sonne“ zu verwenden, weder umgangssprachlich noch gerade in einem Gesetz, wenn dem nicht ein solches Verständnis zugrunde liegen würde!

[188] Siehe Simitis (Petri in: 2011, § 4d, Rn. 32).

[189] Siehe dazu und zum folgenden BVerfG (1983, S. 43).

[190] Das BVerfG hat dieses Recht nicht erfunden, es hat es *nur* zum Grundrecht erklärt. Siehe Seidels „Selbstbestimmungsrecht, Informationen vorzuenthalten oder mitzuteilen“, Seidel (1970, S. 1582 f.), und Steinmüllers „informationelle[s] Selbstbestimmungsrecht“, Steinmüller et al. (1971, S. 93), die es beide schlicht von Westin (1967, S. 7) übernommen haben.

[191] Siehe dazu und zum folgenden auch die Ausführungen in Abschnitt 2.4.2, S. 144.

[192] Siehe schon Steinmüller et al. (1978, S. 86 ff.) sowie Pohle (2015b) und – weil letzteres eine Ausprägung des Problems des fehlenden Verständnisses des Datenschutzrechts für die Folgen komplexer Systeme ist – Pohle (2016c, S. 9).

[193] Am deutlichsten sicher von Simitis (Simitis in: 2011, § 1, Rn. 25). Siehe aber auch die Ausführungen des BVerfG (1983, S. 41 ff.) zur „Selbstbestimmung“, die dort keineswegs nur als „informationelle“ Selbstbestimmung auftaucht, sondern gerade auch als Synonym für die freie Entfaltung der Persönlichkeit des Menschen, der „in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt.“ Diese „[i]ndividuelle Selbstbestimmung“, die die „Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen“ ebenso umfasst wie die tatsächliche Möglichkeit, „sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten“, beschränkt sich gerade nicht nur auf das individuelle Verfügungsrecht über die Informationen und kann durch dieses Verfügungsrecht allein auch nicht geschützt werden. Vielmehr sind es zwei andere durch den Datenschutz, aber nicht das Datenschutzrecht adressierte Problembereiche, die einen signifikanten Einfluss auf die Selbstbestimmung als „elementare[r] Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens“ haben: Informationsfreiheitsrechte gegen Informationsmächtige – oder spiegelbildlich: Transparenzpflichten für Informationsmächtige – und die Verhinderung der Monopolisierungstendenzen bei Gatekeepern über gesellschaftliche Informationsflüsse. Geradezu

unumstritten ist[194] und die Form der Umsetzung im Recht die einer informationellen „Fremdbeschränkung“ ist – einer Beschränkung der Informationsverarbeitung der Normadressatin.[195] Die gesamte gesellschaftliche Ebene der Auswirkungen moderner Informationsverarbeitung durch Organisationen bleibt damit – bis auf singuläre Ausnahmen[196] – außerhalb des Zugriffs des Datenschutzrechts.

3.6.2 Informationsbegriff

Der historisch der Datenschutztheorie zugrunde gelegte Informationsbegriff, der an den der Semiotik angelehnt ist und vier Dimensionen – Syntax, Semantik, Pragmatik, Sigmatik – aufweist, kann, nach der rechtswissenschaftlichen Debatte zu urteilen, nicht als konsentierter Informationsbegriff im Bereich des Datenschutzrechts gelten.[197] Dieser modelltheoretische Informationsbegriff, der Informationen als Modelle von Objekten, also „Abbildungen von etwas für jemand für einen Zweck“[198] fasst und damit alle vier Dimensionen spezifisch für das Recht anknüpfbar macht, wird sehr selten überhaupt dargestellt – und wenn, dann zusammenhanglos oder verkürzt wiedergegeben –,[199] spätestens seit Anfang der 1990er Jahre jedoch nicht mehr zur strukturierten Analyse des Datenschutzproblems genutzt.[200] Die vier Dimensionen sind dennoch immer noch die Ansatzpunkte für die rechtliche Regelung: Informationen unterfallen dem Datenschutzrecht nur, wenn sie sich auf Personen beziehen oder beziehen lassen – sigmatische Dimension –,[201] und erst, wenn sie zeichenmäßig verkörpert werden,[202] an ihre pragmatische Dimension knüpft das

abwegig ist daher die Behauptung von Simitis (Simitis in: 2011, § 1, Rn. 38): „In dem Maße, im [sic!] dem das Recht der Einzelnen garantiert und ausgeübt wird, selbst über die Preisgabe und Verwendung ihrer Daten zu entscheiden, sind auch die Grundbedingungen einer demokratischen Gesellschaft gewährleistet.“

[194] Siehe zur Übersicht Simitis (Simitis in: 2011, § 1, Rn. 46 f.).

[195] Siehe von Lewinski (2014, S. 40 ff., vor allem S. 46 ff.), der bei der Darstellung der verwandten Konzepte an dieser Stelle allerdings das Urheberrecht unterschlägt, obwohl es gerade auch in Form – sehr ausgeprägter – Fremdbeschränkung verrechtlicht ist. Und für das Datenschutzrecht ist diese Konstruktion auch weder überraschend noch dysfunktional, sie ist gerade das historische Produkt eines strukturalistischen – und nicht eines individualistischen – Ansatzes der Problemlösung, siehe Steinmüller (1976c, S. 14).

[196] Siehe § 1 Abs. 1 Nr. 2 Hessisches Datenschutzgesetz, der die Bewahrung des „auf dem Grundsatz der Gewaltenteilung beruhende[n] verfassungsmäßige[n] Gefüge[s] des Staates“ als Aufgabe des Datenschutzes bestimmt, und § 24 Abs. 2, der der Hessischen Datenschutzbeauftragten die Aufgabe überträgt, „die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der datenverarbeitenden Stellen [zu beobachten]. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.“

[197] Was auf den ersten Blick überraschen mag, weil der Begriff *explizit* der ursprünglichen Datenschutzrechtskonzeption zugrunde gelegt wurde, siehe Steinmüller et al. (1971, S. 42 f.), wird vielleicht etwas verständlicher vor dem Hintergrund, dass es trotz jahrzehntelanger Diskussion über Fragen aus dem Feld des Informationsrechts in der Rechtswissenschaft insgesamt keinen konsentierten Informationsbegriff gibt, siehe von Lewinski (2014, S. 5).

[198] Podlech (1976d, S. 22).

[199] Siehe Simitis (Dammann in: 2011, § 3, Rn. 6) für eine solche zusammenhanglose Wiedergabe, die in der Darstellung eigentlich vor Rn. 5 kommen müsste, um sie zu strukturieren, Albers (2002) für eine verkürzte Wiedergabe und etwa Däubler et al. (Weichert in: 2010, § 3, Rn. 2 ff.) für eine schlichte Nichtdarstellung.

[200] Das letzte Beispiel ist wohl Steinmüller (1993). Siehe Kapitel II, S. 155 ff., zur Darstellung des Begriffs der Information mit den vielen, teilweise auch unsystematisch eingestreuten dimensionsspezifischen Problemaspekten, sowie S. 670 ff. zu deren Anwendung auf den „Informationsschutz“.

[201] Siehe die Ausführungen zum Geltungsbereich des Datenschutzrechts.

[202] Siehe Simitis (Dammann in: 2011, § 3, Rn. 5).

datenschutzrechtliche Zweckbindungsprinzip an[203] und mit der semantischen Dimension wird gerade der Kontext adressierbar – einerseits als Erhebungs-, andererseits als Verwendungskontext[204] –, der sowohl die Bedeutung der Information wie auch die Risiken für die Betroffenen (mit-)bestimmt und an den gerade die „bereichsspezifischen" Datenschutzregelungen anknüpfen.[205]

3.6.3 Phasenorientierung

Während die Phasen historisch als Analyseinstrument für die Riskanz der Informationsverarbeitung und zugleich als Anknüpfungspunkt für rechtliche Regelungen vorgesehen waren,[206] haben sie diesen doppelten Charakter schon im Laufe des Gesetzgebungsverfahrens verloren: Das BDSG 1977 beschränkte sich auf einen Schutz von Betroffenen gegen „Mißbrauch" der sie betreffenden Informationen nur in den im Gesetz genannten Phasen – und das hieß eben: innerhalb einer Teilmenge der von Steinmüller et al. in einem ersten Versuch identifizierten Phasen.[207] Erst mit dem Volkszählungsurteil wurde der Gesetzgeber gezwungen, für einen umfassenden Schutz zu sorgen.[208] In der Folge wurden auch die Erhebung und die Nutzung als Phasen ins BDSG integriert. Allerdings kam es an keiner Stelle zu einer grundlegenden Überarbeitung der Phasenaufteilung.

Zwar ist das deutsche Datenschutzrecht immer noch „verarbeitungsorientiert",[209] insoweit dass alle deutschen datenschutzrechtlichen Regelungen die Zulässigkeitsanforderungen jeweils an die einzelnen Phasen stellen, aber diese Phasen sind nicht mehr die zentralen Anknüpfungspunkte für Regelungen zum Umgang mit besonderen Risiken.[210] Stattdessen knüpft das Recht zunehmend an eine Vielzahl konzeptionell unverbundener Einzelaspekte an, die damit zugleich als Topoi besonderer Risiken markiert werden.[211] Dazu gehören etwa die aus dem europäischen ins deutsche Datenschutzrecht übernommenen „besonderen Arten personenbezogener Daten",[212]

[203] Siehe umfassend zum Konzept Hoffmann (1991) sowie zur „Zweckbindung als Kernelement des verfassungsrechtlichen Datenschutzes" BVerfG, Urteil des Ersten Senats vom 20. April 2016 – 1 BvR 966/09 – Rn. 292.

[204] Siehe schon Steinmüller et al. (1971, S. 73). Das BVerfG bezeichnet den Verwendungskontext später als „Verwendungszusammenhang", siehe BVerfG (1983, S. 45), wobei diese Stelle im Urteil durchaus auch so verstanden werden kann, dass das BVerfG damit nicht nur den Kontext, sondern Kontext *und* Zweck meint.

[205] Siehe BVerfG (1983, S. 46) zur verfassungsrechtlichen Begründung der Notwendigkeit solcher bereichsspezifischen Regelungen.

[206] Siehe Steinmüller et al. (1971, S. 57).

[207] Anders aber Woertge (1984, S. 144), der meint, „die Regelung des Bundesdatenschutzgesetzes so auszulegen [sei], daß ab dem Zeitpunkt der Speicherung jegliche Datenverarbeitung erfaßt sein soll", denn „der Katalog der §§ 2 Abs. 2, 1 Abs. 2 BDSG [sei] nicht als abschließend zu verstehen".

[208] Siehe Zilkens (2008, S. 103, Rn. 68).

[209] Siehe Denninger (1987, S. 133).

[210] Nur in einem Zusammenhang fokussiert jedenfalls die wissenschaftliche und politische Diskussion auf die phasenspezifischen Risiken, wenn auch nur im Allgemeinen, nämlich beim Streit um die das Datenschutzrecht prägende Vorverlagerung des Schutzes, siehe zu dieser Prägung BVerfG (2007, S. 184), und dort vor allem im Hinblick auf die zeitliche Vorverlagerung von der Nutzung auf die Erhebung, Speicherung und Verarbeitung. Zu dieser Diskussion siehe schon Miller (1969, S. 1221 i. V. m. 1119 f.).

[211] Das ist im europäischen Datenschutzrecht noch deutlicher als im deutschen, denn das europäische kennt, von den Transparenzpflichten bei der Erhebung nach Art. 13 f. EU-DSGVO, keine phasenspezifischen Zulässigkeitsanforderungen – alles wird unter dem Begriff „Verarbeitung" gefasst, siehe Art. 4 Nr. 2 EU-DSGVO, und im wesentlichen einheitlich geregelt.

[212] Siehe § 3 Abs. 9 BDSG und Art. 9 f. EU-DSGVO. Diese Fehlvorstellung von Sensitivität als intrinsischer Eigenschaft von Informationen ist offensichtlich nicht auszurotten, siehe Simitis (1990), so abstrus sie auch ist, so schon früh Miller (1969, S. 1188 und 1231) und mit Bezug darauf Steinmüller et al. (1971, S. 73).

„automatisierte Einzelentscheidungen“,[213] die Videoüberwachung,[214] der Einsatz „mobiler personenbezogene Speicher- und Verarbeitungsmedien“[215] oder die „Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen“.[216]

3.6.4 Verfahrens- und Technikgestaltung und -prüfung

Das Bundesdatenschutzgesetz war von Anfang an darauf ausgerichtet, sowohl auf die Verfahren wie auch auf die informationstechnischen Systeme gestaltend einzuwirken.[217] Diese Zielvorstellungen wurden allerdings schon in der Startphase – unter anderem durch den Bundesdatenschutzbeauftragten – erfolgreich unterminiert.[218] Erst mit der Novellierung des BDSG 2001 wurde mit dem Grundsatz der Datenvermeidung und Datensparsamkeit in § 3a das Ziel einer datenschutzfreundlichen Verfahrensgestaltung wieder im Gesetz verankert,[219] wobei der Charakter der Norm durchaus umstritten und ihre Durchsetzungsfähigkeit quasi inexistent ist.[220] Im Rahmen der Kontrolle der Rechtmäßigkeit der laufenden Datenverarbeitung ist der Datenschutzbeauftragten aber nach § 4g Abs. 1 Satz 4 Nr. 1 BDSG auch die Kontrolle der „ordnungsgemäße[n] Anwendung der Datenverarbeitungsprogramme“ übertragen, eine Aufgabe, die wohl mehrheitlich als „Kontrolle der Programmgestaltung“ ausgelegt wird,[221] und damit die Einbindung der Datenschutzbeauftragten in die Systemgestaltung erfordert. Auf deren Kritik oder Änderungsforderungen muss die Datenverarbeiterin dabei allerdings ebenso wenig reagieren oder gar eingehen wie im Falle der die Vorgaben des Art. 20 EG-DSRL umsetzenden Vorabkontrolle nach § 4d Abs. 5 und 6 BDSG.[222] Diese Vorabkontrolle ist nach § 4d Abs. 5 immer dann durchzuführen, wenn „automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen“.[223] Mit der EU-DSGVO wurde die Vorabkontrolle durch die Datenschutz-Folgenabschätzung nach Art. 35 ersetzt, allerdings nur mit sehr allgemeinen Vorgaben hinsichtlich der Anforderungen an die Durchführung und den Umfang.[224] Das Datenschutzaudit nach § 9a BDSG, zu dem der Bundesgesetzgeber nie ein Ausführungsgesetz erlassen hat, geht nicht wesentlich über das hinaus, was eine Vorabkontrolle, eine Programmkontrolle und Rechtmäßigkeitskontrolle auch schon bieten,[225] wird allerdings durch unabhängige externe

[213] Siehe § 6a BDSG und – zusammen mit dem Profiling – Art. 22 EU-DSGVO.
[214] Die „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“, siehe § 6b BDSG.
[215] Siehe § 6c BDSG.
[216] Siehe Art. 44 ff. EU-DSGVO.
[217] Siehe schon zu dieser Zielvorstellung Müller (1975a, S. 123) und Steinmüller (1976c, S. 12) sowie zum ersten Versuch einer breit angelegten Umsetzung Steinmüller et al. (1978).
[218] Siehe Pohle (2015a).
[219] Siehe Simitis (Scholz in: 2011, § 3a, Rn. 34), der hingegen behauptet, dieses Ziel sei erstmalig im Gesetz verankert worden.
[220] Siehe umfassend von Stechow (2005, S. 86 ff.).
[221] So jedenfalls Simitis (Simitis in: 2011, § 4g, Rn. 43) und Däubler et al. (Däubler in: 2010, § 4g, Rn. 15), je mit weiteren Nachweisen.
[222] Siehe Simitis (Petri in: 2011, § 4d, Rn. 37). Das liegt nicht unerheblich daran, dass das Ergebnis der Vorabkontrolle „(nicht öffentlicher) Bestandteil des Verfahrensverzeichnisses“ wird, siehe Zilkens (2008, S. 159, Rn. 149), und es damit an – aus der Transparenz resultierendem – Druck mangelt. Zu den möglichen Folgen etwa in Haftungsfällen siehe aber auch Simitis (Petri in: 2011, § 4d, Rn. 41).
[223] Siehe dazu, zu den Umsetzungen in den Landesdatenschutzgesetzen und zur Kritik Friedewald et al. (2016, S. 8 f.).
[224] Siehe Friedewald et al. (2016, S. 15 f.). Siehe zum Vergleich die hinsichtlich der abgedeckten Bedrohungen weit umfassendere Analyse im Rahmen eines Surveillance Impact Assessment bei Wright und Raab (2012), die noch über das bei Friedewald et al. (2016, S. 29 ff.) vorgestellte „alternative[] Verfahren für wissenschaftliche Datenschutz-Folgenabschätzungen“ hinausgeht.
[225] Siehe die Darstellung bei Simitis (Scholz in: 2011, § 9a, Rn. 2 ff.).

Gutachterinnen durchgeführt und – für Schutzkonzepte, Verfahren oder Produkte – mit einem „Qualitätsnachweis[] (z. B. Siegel, Zertifikat oder Auditzeichen)“ belohnt. In der EU-DSGVO wird dieses Verfahren als „Zertifizierung“ bezeichnet und in Art. 42 geregelt. Auch die Technikgestaltung – „Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default)“[226] – selbst ist nach langer Diskussion inzwischen auch auf europäischer Ebene – in Art. 25 EU-DSGVO – geregelt worden, wobei die Regelung die Erwartungen, die von vielen Seiten in sie gesteckt wurden und werden, wohl nicht erfüllen wird.[227]

3.6.5 Schlussfolgerungen

Aus der Darstellung des für die Technikgestaltung relevanten Verhältnisses zwischen dem Datenschutz und dem geltenden Datenschutzrecht lassen sich nun einige Schlussfolgerungen ziehen.

Zwar überschneiden sich die Geltungsbereiche von Datenschutz und Datenschutzrecht, sie sind jedoch weder deckungsgleich, noch ist eines eine Teilmenge des je anderen. Der Schutzbereich des Datenschutzrechts ist signifikant kleiner als der des Datenschutzes, zugleich ist der Kreis der Normadressatinnen des Datenschutzrechts signifikant größer. Gleichwohl lässt sich feststellen, dass für Organisationen als Informationsverarbeiterinnen der Schutzbereich des Datenschutzes eine Obermenge des Schutzbereiches des Datenschutzrechts ist. Damit ist grundsätzlich eine datenschutzfreundliche Informationsverarbeitung durch Organisationen auch eine datenschutzrechtskonforme, eine datenschutzrechtskonforme jedoch nicht notwendig datenschutzfreundlich. Die Betroffenen im Sinne des Datenschutzrechts würden demnach in jedem Fall davon profitieren, wenn die Datenschutztheorie als Instrument für die Analyse der Risiken und Bedrohungen, die von Organisationen ausgehen, zum Einsatz käme.

Sowohl hinsichtlich des Informationsbegriffs wie hinsichtlich der Phasenorientierung zeigt das bestehende Datenschutzrecht Defizite, die sich sowohl auf seine Weiterentwicklung wie auch auf seine Anwendung in der Praxis beschränkend auswirken. Die praktische Anwendung des bestehenden Rechts würde damit sowohl im Hinblick auf eine fundierte Bedrohungsanalyse als auch im Hinblick auf die Verfahrensgestaltung von der Verwendung des modelltheoretischen Informationsbegriffs der Datenschutztheorie wie auch vom phasenorientierten Analyseansatz deutlich profitieren, etwa indem die Abwehr der identifizierten, phasenspezifischen Bedrohungen in den datenschutzrechtlichen Abwägungsprozess als Teil der berechtigten Interessen der Betroffenen aufgenommen würde.

Soweit es hinsichtlich der Prüfungen – Folgenabschätzungen und Audits – und der Gestaltungen – Verfahren und informationstechnische Systeme – an konkreten gesetzlichen Anforderungen zu Umfang und Durchführung – und bei den Prüfungen auch zum Umgang mit dem Ergebnis – mangelt, ist der oben vorgelegte Operationalisierungs- und Regelungsansatz voll anschlussfähig, ohne jedoch die Lücken bei den Transparenzpflichten füllen zu können. Nur damit ließen sich aber sowohl die Qualität von Prüfungen und Technikgestaltungsprozessen wie auch die Bindungswirkung der dabei getroffenen Entscheidungen, etwa zur Zwecksetzung, steigern.

[226] EU-DSGVO, Erwägungsgrund 78.

[227] Siehe schon die Kritik bei Hornung (2012, S. 103), wenn auch noch zur Fassung des Entwurfs, deren Formulierung weitgehend der von § 9 BDSG entsprach. Die einzige relevante Änderung der verabschiedeten Fassung gegenüber dem Entwurf betrifft die Qualifizierung der zu treffenden Maßnahmen durch „wie z. B. Pseudonymisierung, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen“. Genau das ergab sich aber eben schon aus der Regelung im Entwurf, denn die Datenschutzgrundsätze sind nämlich gerade Teil der „Anforderungen dieser Verordnung“. Siehe auch kritisch Pohle (2015a, S. 43).

4 Die Technik des Datenschutzes

Ausgehend von den im zweiten Kapitel dargestellten Ergebnissen der jahrzehntelangen wissenschaftlichen Auseinandersetzungen um *privacy*, Datenschutz und *surveillance* und auf der Basis des im dritten Kapitel rekonzeptionalisierten Datenschutzes werden nun Folgerungen für die Gestaltung datenschutzfreundlicher – und dabei nicht notwendig nur datenschutzrechtskonformer – informationstechnischer Systeme als Teilkomponenten von soziotechnischen Systemen gezogen.

4.1 Vorbemerkungen

Erstens: Nachdem die Arbeit gezeigt hat, dass fast alle in der Vergangenheit vorgeschlagenen komplexitätsreduzierenden Entscheidungshilfen – die Trennung von „privat“ und „öffentlich“, die Sphärentheorie, die „Sensitivität“ von Informationen, ja sogar die personenbezogenen Informationen – strukturell untauglich sind, bleibt eigentlich nur, mit Winston Churchill zu sagen „I have nothing to offer but blood, toil, tears and sweat“, und bis zur Entwicklung neuer – und dann hoffentlich geeigneter – Komplexitätsreduktionsmechanismen den langen und beschwerlichen Weg zu gehen und im Rahmen jeder Systementwicklung ein umfassendes *wissenschaftliches* Impact Assessment durchzuführen, wie es für den Datenschutz im vorherigen Kapitel in Form eines prozeduralen Operationalisierungsansatzes vorgelegt wurde.[1]

Zweitens: Das Modellieren ist keine formale Tätigkeit,[2] gerade auch dort nicht, wo gesellschaftliche Realitäten mit ihren sozial ausgehandelten Normen, ihren Kompromissen, aber auch ihren offenen und verdeckten Konflikten und den sie prägenden Machtstrukturen modelliert werden sollen. Es ist nicht unwahrscheinlich, dass dies nirgends mehr gilt als im Bereich von *privacy*, Datenschutz und *surveillance*. Nicht nur beschreibt so gut wie jede der in diesem Bereich operierenden Theorien das Feld als konfliktgeladen und geprägt von Interessengegensätzen, in dem erbitterte Auseinandersetzungen zwischen Datenverarbeiterinnen, Betroffenen und all den anderen streitbaren Geistern geführt werden, auch viele Vertreterinnen der unterschiedlichen Theorien tragen nicht unbedingt dazu bei, die Diskussion zwischen den Theorien zu einem Vorbild für eine Habermas'sche herrschaftsfreie Kommunikation zu machen.

Drittens: Aufgabe der Informatik in Bezug auf den Datenschutz ist keineswegs nur die Gestaltung technischer (oder die Mitgestaltung soziotechnischer) Systeme zur Verbesserung der Durchsetzung des Datenschutzes, sondern vor allem, die Grenzen von technischen Lösungen und der Lösbarkeit durch Technik im Allgemeinen gegenüber den Datenverarbeiterinnen, den Betroffenen und der Gesellschaft insgesamt transparent zu machen – und damit grundsätzlich verhandelbar. Insoweit es sich beim Datenschutzproblem in erster Linie um ein Gesellschaftsproblem und nicht um ein Technikproblem handelt, ist der in der Informatik weitverbreitete

[1] Siehe zur Qualifizierung als wissenschaftlich Friedewald et al. (2016, S. 21 f.). Siehe dazu auch schon Rost und Bock (2012, S. 744 f.). Der damit zwangsläufig einhergehende Aufwand hat strategisch den Vorteil, genug Zwang auf alle beteiligten Akteurinnen – Wissenschaftlerinnen, Entwicklerinnen sowie den Gesetzgeber – auszuüben, dass die Wahrscheinlichkeit für eine Entwicklung geeigneter Komplexitätsreduktionsmechanismen steigt.

[2] Siehe dazu und zum folgenden umfassend Coy (1992), eine Entwicklung in dieser Richtung fordert aber etwa van Lamsweerde (2008).

„solutionism“ (Evgeny Morozov) mehr als nur unpassend – er ist gefährlich, denn er suggeriert eine Lösung, wo es prinzipiell keine geben kann.

Viertens: Technikentwicklung muss als Rückmeldung liefern, welche Auswirkungen die Technik auf die Machtstruktur hat. Wenn das zu entwickelnde System zu komplex ist, um die Folgen für die Machtstruktur zu analysieren, dann ist es zu komplex, um es zu entwickeln.[3]

Fünftens: Die Gestaltung von Informationssystemen soll sich, Heinz von Foerster folgend, an dem Ziel ausrichten, neue Möglichkeiten – und damit mehr Freiheit – zu erzeugen. Ein zentraler Schutzmechanismus für Freiheit ist Kontingenz,[4] die auf der technischen Ebene etwa dadurch erreicht werden kann, dass zwar die Datenverarbeiterinnen die Technik gestalten, die „Konfigurationsmacht“ jedoch auf Seiten der Betroffenen liegt.[5] Freiheitsbeschränkungen hingegen ergeben sich oft schon als Folge von beschränkenden Prozessen, die selbst historische Produkte konkreter – und damit je spezifisch beschränkter – Techniken sind (Akten, Ausweise mit Geburtsdaten). Ein wesentlicher Lösungsansatz besteht in der Übertragung der Funktion im Gegensatz zu einer Übertragung der überkommenen Prozesse (Geschirrspüler gegen Handspülroboter).

Sechstens: Dieses Ziel muss selbstreflexiv auf die Technik selbst bezogen werden. Die Technik ist so zu gestalten, dass sie in Zukunft wieder umgestaltet werden kann. Ein Beispiel für eine solche „Technik“ ist der Rechtsstaat: Er stellt die Mittel bereit, um ihn selbst infrage stellen zu können. Informationstechnische Systeme müssen das auch können:[6] ein „Not-Aus“-Schalter für Machtmaschinen, wie es sie in den meisten Kraftmaschinen schon gibt.

Siebtens: Als konzeptionelles Gegenstück zur Kontingenz zugunsten der Betroffenen sind informationstechnische Systeme, die unter der Kontrolle der Organisationen stehen, mit technischen Vertrauensankern zu versehen, um einerseits selbst- und Fremdkontrolle sicherzustellen, andererseits aber auch Intervenierbarkeit durch die Betroffenen schon auf der technischen Ebene zu ermöglichen und ihnen damit Interventionsmöglichkeiten zu bieten, ohne auf die Kooperation der Organisationen angewiesen zu sein.

4.2 Technikgestaltung und Datenschutz

Datenschutzkonformität und Datenschutzrechtskonformität sind Eigenschaften von Informationsverarbeitungspraxen, nicht von Technik.[7] Technik soll *datenschutzfeindlich* heißen, wenn sie nicht datenschutzkonform eingesetzt werden kann, wenn sie also Datenschutz verhindert. Sie

[3] Siehe Podlech (1982).

[4] Siehe schon Steinmüller (1975a, S. 524, Fn. 43).

[5] Damit ist deutlich mehr gemeint als nur die Auswahl von Farben – es geht um einen tatsächlichen Machtverlust für Organisationen und einen Machtgewinn für Betroffene. Es reicht nicht aus, dass Software auf den Geräten der Betroffenen läuft, denn der Ort selbst impliziert nicht, wer die Herrschaft hat – die Organisation oder die Betroffene –, wie sich etwa an DRM-Systemen zeigt. Systeme, die nicht von den Betroffenen beherrscht werden, befinden sich rechtlich im Herrschaftsbereich der Organisation mit der Folge, dass die Organisation zur verantwortlichen Stelle wird, wenn die Software personenbezogene Informationen verarbeitet. Für einen Vorschlag zu einem solchen System verteilter Kontrolle – und damit Macht – siehe Rost (2008b). Siehe auch Spiekermann und Cranor (2009) für eine konzeptionell etwas beschränktere, weil nur auf personenbezogene Informationen fixierte, Darstellung auf der Basis von drei Einflusszonen, einer „user sphere“, einer „recipient sphere“ und einer „joint sphere“.

[6] Siehe Hildebrandt (2008, S. 177 f.).

[7] Nicht nur Menschen und Organisationen tendieren dazu, ihre Anforderungen an informationstechnische Systeme in Form von Anforderungen an Handlungen oder Praxen, die von oder mit diesen Systemen vorgenommen werden sollen, zu formulieren, siehe schon Antón (1996), sondern auch das Recht. Siehe etwa zur Verarbeitungsorientierung des Datenschutzrechts Denninger (1987, S. 133) sowie dazu, dass das Recht an soziale Akteurinnen, nicht an Maschinen gerichtet ist, Bull (1983, S. 21). Bruce Schneiers berühmtes Diktum „Se-

heiße *datenschutzunfreundlich*, wenn sie einen datenschutzkonformen Einsatz behindert oder erschwert. Technik heiße *datenschutzneutral*, wenn die Datenschutzkonformität nur von der Art und Weise des konkreten Einsatzes abhängt. Sie heiße *datenschutzfördernd*, wenn sie einen datenschutzkonformen Einsatz unterstützt und einen nicht datenschutzkonformen erschwert. Und Technik heiße *datenschutzgarantierend*, wenn sie unabhängig von der Intention der Datenverarbeiterin ausschließlich datenschutzkonform eingesetzt werden kann.

In dem Feld zwischen datenschutzfördernd und datenschutzgarantierend und vor dem Hintergrund von – gerade auch rechtlichen – Verantwortungszuschreibungen ließe sich darüber hinaus unterscheiden zwischen (1) einfachen Unterstützungssystemen, die etwa Entscheidungshilfe bieten, (2) Systemen, die nicht unbewusst umgangen werden können, (3) Systemen, die weder unbewusst noch fahrlässig umgangen werden können, und (4) Systemen, die gar nicht – auch nicht vorsätzlich – umgangen werden können.

Eine solche Klassifikation ermöglicht interdisziplinäre Anschlussfähigkeit nicht nur in der Wissenschaft, sondern auch in der Praxis, etwa zwischen Informatik und Recht. Ein Beispiel: Derzeit besteht ein extremes Vollzugsdefizit im Datenschutzbereich. Die Datenschutzbehörden haben Schwierigkeiten, vorsätzlich begangene Datenschutzverstöße angemessen zu ahnden, denn die Täterinnen können damit rechnen, dass sie sich erfolgreich herausreden können, weil den Behörden die Ressourcen fehlen, um den Vorsatz nachweisen zu können. Im Ergebnis sehen sich die Behörden gezwungen, die Ausreden akzeptieren zu müssen, um wenigstens die oft sehr viel geringeren Strafen oder Bußgelder für fahrlässig begangene Datenschutzverstöße verhängen zu können. Weil in der Folge die Profite die Strafen um Größenordnungen übersteigen, ist das für vorsätzlich agierende Täterinnen ein Anreiz, den Datenschutz einfach komplett zu ignorieren, vor allem weil darüber hinaus die Entdeckungswahrscheinlichkeiten marginal sind. Die Informatik kann das ändern.[8] Wenn Informatikerinnen für konkrete Systeme nachweisen können, dass sie in die vorgenannte Klasse 3 fallen, dann kann das Recht darauf durch die Umkehr der Beweislast reagieren. In der Folge muss nicht mehr denjenigen, denen ein Datenschutzverstoß nachgewiesen wird, auch Vorsatz nachgewiesen werden, sondern der Vorsatz wird unterstellt. Jetzt müssen die Beschuldigten nachweisen, dass es kein Vorsatz war. Und wenn ihnen das nicht gelingt, dann können die Aufsichtsbehörden signifikant höhere Strafen verhängen. Technik kann insofern die Rolle eines „Ausreden-Terminators“ spielen.[9]

Nun kann eingewandt werden, dass die Technik ihren eigenen Einsatz nicht erzwingen kann. Das ist korrekt, und das ist einer der Gründe, warum viele Versuche, datenschutzgarantierende Technik zu gestalten, im Grunde nichts weiter als akademische Spielereien sind. Aber auch dieses Problem kann das Recht lösen. Während nämlich Technik nur berechenbare Probleme lösen kann, kann Recht sogar unlösbare lösen:[10] Wenn es genügend Klasse-3-Systeme gibt, dann kann Recht die Beweislast auch umkehren, wenn die Beschuldigten ein solches System nicht einsetzen.

curity is a process, not a product“, Schneier (2004, S. 84), lässt sich also auf den Datenschutz übertragen: Datenschutz ist ein Prozess, kein Produkt.

[8] Auch der Gesetzgeber könnte dieses Problem relativ einfach lösen, etwa durch die allgemeine Einführung einer Gefährdungshaftung, wie es sie bisher nur bei Datenschutzverstößen durch öffentliche Stellen gibt, siehe § 8 BDSG. Ich danke Kai von Lewinski für diesen Hinweis.

[9] Das hat durchaus Ähnlichkeit mit den möglichen Folgen eines Ignorierens der Stellungnahme einer Datenschutzbeauftragten im Anschluss an eine Vorabkontrolle und der darin enthaltenen Empfehlungen durch die verantwortliche Stelle, siehe Simitis (Petri in: 2011, § 4d, Rn. 41), allerdings geht der hier vorgelegte Vorschlag viel weiter.

[10] Siehe etwa Luhmann (1969). Zugegeben, es handelt sich ein wenig um ein Sprachspiel mit dem Begriff „lösen“, aber eben nur ein wenig. Niemand käme auf die Idee, das strafrechtliche Mordverbot scheitere, weil es die abgeschossene Kugel nicht aufhalten könne. Das ist korrekt, aber Recht wirkt auch nicht auf Dinge, sondern

In dem Fall müssen dann die Beschuldigten nachweisen, dass es auch zu einem Verstoß gekommen wäre, wenn sie ein solches System eingesetzt hätten.

Hier zeigt sich, dass Probleme im Bereich des Datenschutzes, die sich in keiner einzelnen der beteiligten Disziplinen lösen lassen, lösbar sind, wenn die Disziplinen kooperieren. Und da es – wahrscheinlich um Größenordnungen – leichter ist, Klasse-3-Systeme zu entwickeln als Klasse-4-Systeme, wird darüber hinaus das Leben für die Entwicklerinnen auch einfacher.

4.2.1 Dokumentation

Dokumentation ist zweifellos eines der Lieblingsthemen der Informatik. Die Forderung nach Verbesserung der Dokumentation wird wahrscheinlich sogar öfter erhoben als die Forderung nach mehr Speicher, und dabei steigt der Bedarf nach Dokumentation sicher nicht in gleichem Maße wie der Bedarf nach Speicher. Die Wahrheit ist: Dokumentation ist unbeliebt, wird vernachlässigt und ist, selbst wenn sie existiert, allzu oft schlicht dysfunktional. Dennoch sprechen einige Gründe für eine umfassende Dokumentation, gerade bei der Entwicklung von IT-Systemen als Teil von soziotechnischen Systemen, die mindestens datenschutzfördernd sein sollen, vor allem wegen des dezidiert interdisziplinären Hintergrunds des Datenschutzes.

Der erste wichtige Grund ist, dass Dokumentation unabdingbar ist, um sicherzustellen, dass die Kommunikation zwischen den Disziplinen erfolgreich verläuft. Dokumentation ist schriftliche Kommunikation, die es erleichtert, frühere Festlegungen neu aufgreifen zu können, wenn sich – was in interdisziplinärer Kommunikation der Standardfall ist – herausstellt, dass der vermeintliche Konsens schlicht das Produkt eines inhaltlichen Missverständnisses auf der einen, der anderen oder auf allen Seiten war.

Der zwingendste Grund für eine Dokumentation ist nicht der Datenschutz, sondern das Datenschutz*recht*. Das Datenschutzrecht ist in weiten Teilen genauso bürokratisch wie die rationale Organisation, die es versucht, unter Kontrolle zu bringen. Und der zentrale Anknüpfungspunkt für die rechtlichen Kontrollmechanismen ist die Dokumentation über das, was kontrolliert werden soll. Das Problem, das daraus entstehen kann, ist offensichtlich: Die Dokumentation ersetzt das, was dokumentiert wird oder werden soll, und das Ausfüllen von Checklisten ersetzt die inhaltliche Auseinandersetzung mit dem, worauf die Checkliste eigentlich nur verweisen soll. Andererseits ist genauso offensichtlich, dass sich nicht prüfen lässt, ob und wie sich eine Entwicklerin mit inhaltlichen Fragen auseinandergesetzt sowie Wertungen und Abwägungen vorgenommen hat, denn im Ergebnis – der Technik – sind der Prozess der inhaltlichen Auseinandersetzung, die Maßstäbe der Bewertungen und die Reflexionen der Abwägungen gerade unsichtbar und unsichtbar gemacht worden.

Eine Dokumentation ist gerade auch dann unabdingbar, wenn sich im Zuge eines Entwicklungsprozesses herausstellt, dass die aus Informatiksicht und vor dem Hintergrund, dass das Ziel darin besteht, Individuen, Gruppen, Organisationen, das staatliche Institutionengefüge und die Gesellschaft insgesamt vor informationsmächtigen Organisationen zu schützen, getroffenen Entscheidungen für oder gegen konkrete zu implementierende Technikeigenschaften gerade mit dem Recht kollidiert. Recht ist dynamisch; es ändert sich mit der Gesellschaft, in der es wirkt. Und einer der zentralen Auslöser solcher Veränderungen ist Dissidenz – *begründete* Dissidenz.

Während die vorgenannten Punkte auf eher nicht aus der Informatik selbst stammende Begründungen für eine umfassende und – auch für Dritte – nutzbare Dokumentation verweisen,

auf soziale Akteurinnen. Recht versucht nicht, die Kugel aufzuhalten, sondern den Menschen vom Schießen abzuhalten.

erzeugt die Informatik gerade im Zuge jeder Verfahrens- und Technikgestaltung einer der zentralen Probleme: das Modellierungsproblem. Und damit fällt der Informatik eben auch die Verantwortung zu, dieses Problem der expliziten oder impliziten, der offenen oder versteckten Modellannahmen zu einem sozial aushandelbaren zu machen, indem sie das Problem transparent macht.

4.2.2 Stakeholder-Einbindung

Eine der Funktionen des Datenschutzes ist die der Produktion von gesellschaftlicher Akzeptanz von organisierter Informationsverarbeitung und deren Industrialisierung, der Schaffung von Systemvertrauen und mithin der Gewährleistung der Akzeptabilität der Informationsgesellschaft.

Die Frage ist, ob dafür die Partizipation der Betroffenen an der Systementwicklung ein geeignetes oder gar erforderliches Mittel ist. Die Antwort hängt davon ab, welchem Akzeptabilitätsbegriff mensch folgt, einem subjektiven oder einem objektiven. Der subjektive Akzeptabilitätsbegriff ist dabei verwandt mit dem demokratischen Prinzip: Akzeptabel ist, was von den Beteiligten akzeptiert wird – *la volonté des tous*. Der objektive Akzeptabilitätsbegriff folgt hingegen dem republikanischen Prinzip mit seiner *volonté générale*.

Wird dem ersten Prinzip gefolgt, dann ist eine Einbindung der Betroffenen unumgänglich, etwa durch partizipative Systemgestaltung. Wird hingegen dem zweiten Prinzip der Vorzug eingeräumt, dann bedarf es einer entsprechenden Rollenzuweisung an ein kompetentes Mitglied des Entwicklerinnenteams.

Beide Ansätze sind nicht unproblematisch. Im ersten Fall kann der Beitrag der Betroffenen nicht von „falschem Bewusstsein“ unterschieden werden,[11] im zweiten Fall kann die Verselbständigung der Stellvertretung nicht verhindert werden.[12]

Wie immer die Entscheidung lautet, sie muss getroffen und begründet werden.

4.2.3 Auswahl des Referenzrahmens

Der wichtigste – oder zumindest der folgenschwerste – Schritt bei der Auswahl zu verwendender und der Gestaltung neuer Technik ist die Entscheidung über den benutzten Referenzrahmen: Welche *privacy*-, *surveillance*- oder Datenschutztheorie oder welches Recht soll als Bezugspunkt gelten? Wegen seines Geltungs- und Befolgungsanspruchs ist Recht grundsätzlich begründungsfrei – in einer bürgerlichen Rechtsordnung wird nur Rechtstreue verlangt –, aber die Frage, welches Recht – und vielleicht sogar: welche Rechtsordnung – einschlägig ist und deshalb angewendet werden muss, ist gerade nicht immer leicht zu beantworten. Hinsichtlich der Theorien ist das einfacher: Jede kann genommen werden, denn keine erzwingt ihre Verwendung. Aber welche auch immer gewählt wird, die Entscheidung muss transparent gemacht und begründet werden. Das folgt schon aus dem aus Systemtheorie und Kybernetik folgenden Verständnis[13] von System, Systemanalyse und Systemgestaltung: Alle drei basieren darauf, dass – ob vom System selbst, von einer Analystin oder, wie hier, von einer Gestalterin – eine Grenze zwischen

[11] Siehe dazu Marx und Engels (1974, Bd. 3, „Die deutsche Ideologie“, S. 26 ff.) und Marx und Engels (1974, Bd. 4, „Das kommunistische Manifest“, S. 478 ff.). Raab und Bennett (1998, S. 271 ff.) geben das sogar offen zu, wollen davon aber gleichwohl nicht lassen.

[12] Siehe dazu Sofsky und Paris (1994). Daran ändert auch die Einbindung von Datenschutzbeauftragten nichts, denn auch sie vertreten in erster Linie sich selbst und ihre eigenen Interessen, insbesondere das Interesse an Selbsterhaltung.

[13] Siehe dazu Heylighen und Joslyn (2001).

System und Umwelt gezogen wird. Es gibt keine „natürliche“ Grenze; Grenzziehung ist Entscheidung und Entscheidung ist – vor allem in der Wissenschaft – begründungsbedürftig. Und die Begründungpflicht trifft die Gestalterin. Und eine sinnvolle Begründung kann sich nur auf die Angemessenheit der gewählten Theorie für den Bereich der sozialen Welt, für den die Technik ausgesucht oder entwickelt oder in dem sie wahrscheinlich eingesetzt wird, stützen. Das heißt, dass das Recht oder die Theorie ausgewählt werden muss, deren Geltungsbereich am ehesten dem zukünftigen Anwendungsbereich der Technik entspricht.

Neben dem Geltungsbreich gehört auch der Schutzbereich, also die Menge der Schutzgüter, zum Referenzrahmen, über den zu entscheiden ist. Während die Theorien tendenziell je einen konsentierten Schutzbereich mitbringen, kann ein konkretes Gesetz, etwa das Bundesdatenschutzgesetz oder die EU-Datenschutzgrundverordnung, unterschiedlich ausgelegt werden.[14] Die unterschiedlichen Auslegungen können dabei – und hier schließt sich der Kreis zwischen Theorien und Recht – gerade wieder den Theorien entsprechen, die es in diesem Feld gibt.[15] Während die Theorien einander grundsätzlich auf Augenhöhe gegenüberstehen und keine der Theorien jeweils ein Primat gegenüber allen anderen geltend machen kann, es sei denn, sie versammelt eine Mehrheit von Wissenschaftlerinnen eines Feldes hinter sich,[16] gibt es im Bereich des Rechts durchaus jeweils „gewichtigere“ oder „weniger gewichtige“ Auslegungen. So sind etwa – jedenfalls in ihren jeweiligen Rechtsräumen – Höchst- oder Verfassungsgerichte legitime Letztauslegungsinstanzen, sie kreieren die „herrschende Meinung“, können sie aber auch wieder ändern – und sie ist immer politisch.[17] Die Entscheidung für eine Theorie oder eine Rechtsauslegung, ja schon für einen Rechtsraum,[18] ist im Hinblick auf den Schutzbereich daher immer eine immanent politische, keine rein wissenschaftliche. Und auch diese Entscheidung muss begründet werden.

Aus dem gewählten Referenzrahmen folgt in weiten Teilen das weitere Vorgehen bei der Analyse der Bedrohungen sowie der Gestaltung und der Auswahl informationstechnischer Systeme, sowohl hinsichtlich des Prozesses, etwa weil Theorien ihre eigenen Vorgehensmodelle mitbringen oder das Recht eine bestimmte Prüfreihenfolge verlangt, wie auch im Hinblick auf die inhaltliche Ausgestaltung der einzelnen Prozessschritte.

[14] Das ist nicht überraschend, denn ein Streit über den Schutzbereich würde bei Theorien tendenziell zu einer Spaltung führen. Hingegen ist das Recht jeweils von außen, nämlich vom Gesetzgeber, vorgegeben und muss damit von allen, die es auslegen, Anknüpfungspunkt bleiben. Siehe dazu grundsätzlich Hirschman (1970).

[15] Siehe gerade die Darstellung bei von Lewinski (2014, S. 17 ff.). Die dort dargestellten Schutzgüter sind in der übergroßen Mehrzahl solche, die mit außerrechtlichen Theorien begründet werden, und für die von Lewinski dann nach einer Verortung im Recht sucht. Und erst diese Verortung im Recht macht aus Schutzgütern *rechtlich geschützte Schutzgüter*.

[16] Zwar lässt sich für verschiedene Theoriefragmente, wie etwa die Fixierung auf personenbezogene Informationen oder das Primat der Informationsflusskontrolle durch die Betroffenen, durchaus konstatieren, dass es dafür jeweils Mehrheiten gibt, aber bisher ist es offensichtlich keiner Theorie gelungen, sich selbst als die Theorie der Mehrheit durchzusetzen. Und schon beim Primat der Informationsflusskontrolle durch die Betroffenen wird deutlich, dass dieses Primat in unterschiedlichen Theorien ganz unterschiedlich gehandhabt wird – in einigen Theorien tritt es als Teil des Kerns der Theorie selbst auf – also als Schutzgut –, in anderen ist es nur der vorgeschlagene Regelungsansatz, mit dem die eigentlichen Schutzgüter geschützt werden sollen.

[17] Siehe instruktiv auch für Nichtjuristinnen Wesel (1979).

[18] Es ist nämlich keineswegs „natürlich“, dass ein globales Problem wie das *privacy*-, Datenschutz- und *surveillance*-Problem auf der Basis des deutschen oder europäischen Rechtsverständnisses gelöst werden soll.

4.2.4 Privacy-Enhancing Technologies

Alle bestehenden PETs[19] sind auf der Basis von Annahmen über die Akteurskonstellation, die Schutzgüter und die Bedrohungen für diese Schutzgüter entwickelt worden. Das gleiche gilt für die Vorschläge für noch zu entwickelnde PETs. Nicht immer wurden und werden diese Annahmen dabei expliziert.[20] Bevor für ein Entwicklungsprojekt ein bestehendes oder zu entwickelndes informationstechnisches System als Bauteil ausgewählt wird, ist daher immer zu bestimmen, welche Annahmen der betreffenden Systemgestaltung zugrunde gelegt wurden. Für die nicht mit den Annahmen des für das eigene Entwicklungsprojekt gewählten Referenzrahmens übereinstimmenden Annahmen ist dann insbesondere zu prüfen, welche Nebenwirkungen bei einem Einbau oder Einsatz dieses Bauteils auftreten können und wie mit diesen umgegangen werden soll, also wie sie etwa entschärft werden sollen oder ob sie ignoriert werden können. In jedem Fall ist die Entscheidung zu begründen und transparent zu machen. Die Aufdeckung der zugrunde gelegten Annahmen für bestehende PETs bietet zugleich eine Möglichkeit, den Lösungsraum insgesamt transparent zu machen und strukturelle Lücken zu identifizieren.[21] Damit werden zugleich die strukturellen Lücken in der Schutzabdeckung gesellschaftlich diskutierbar.

Für einige Anwendungsbereiche sind wenigstens große Teile der Annahmen bereits expliziert und transparent gemacht – jedenfalls in der betreffenden Fach-Community, teilweise auch darüber hinaus. So ist etwa, wie im zweiten Kapitel gezeigt, für die Anonymitätsdiskussion im Datenbankenbereich in der informatischen *privacy*-, Datenschutz- und *surveillance*-Forschung allgemein bekannt, dass die Betreiberin der Datenbank in dieser Diskussion nicht als Angreiferin verstanden wird. Auch für Kommunikationssysteme werden fast ausschließlich externe Lauscherinnen oder die Betreiberinnen der Kommunikationsnetze als Angreiferinnen betrachtet. Und für die als PETs im engeren Sinne verstandenen Systeme[22] wird als Ziel formuliert, „unnecessary or unwanted processing of personal data“ zu verhindern, „all without losing the functionality of the information system.“[23] Da es aber nur wenige Arbeiten gibt, in denen die unterschiedlichen Annahmen verschiedener Theorien, die sich mit diesen Anwendungsbereichen beschäftigen, zusammengetragen und zueinander in Bezug gesetzt werden,[24] und es darüber hinaus einen besonderen Mangel an bereichsübergreifenden Arbeiten gibt, wird es beim derzeitigen Stand der Forschung einem Entwicklungsprojekt schwerfallen, auf der Basis des gewählten Referenzrahmens passende technische Lösungen zu finden. Noch defizitärer ist die Situation bei Arbeiten, die disziplinübergreifend anschlussfähig sind und damit sowohl die nichtinformatischen Vertreterinnen der einzelnen Theorien als auch die Juristinnen in ihrer Arbeit am Recht über den Stand der technischen Umsetzungen informieren können.

[19] Hier sollen PETs in einem weiten Sinne verstanden werden als alle informationstechnischen Systeme, die zur technischen Lösung von *privacy*-, Datenschutz- und *surveillance*-Problemen oder Teilbereichen davon dienen sollen.

[20] Siehe die frühe Kritik von Leib (1985) an der fehlenden Explikation der Annahmen in der Datenschutzdebatte.

[21] Als Lösungsraum soll dabei derjenige Teilbereich der Vereinigung der Geltungs- und Schutzbereiche aller *privacy*-, Datenschutz- und *surveillance*-Theorien und -Gesetze bezeichnet werden, für den technische Lösungen existieren, die die jeweils identifizierten Bedrohungen abwehren, entschärfen oder handhabbar machen oder – positiv formuliert – die die definierten Gestaltungsziele erreichen.

[22] Siehe van Rossum et al. (1995).

[23] So die Definition bei van Blarkom et al. (2003, S. 3).

[24] Siehe etwa Gürses (2010) für den Bereich der anonymen Kommunikationssysteme.

4.2.5 Datenschutzfördernde Technikgestaltung

Wenn als Referenzrahmen der im vorherigen Kapitel rekonzeptionalisierte Datenschutz dient, kann dem Vorgehen bei der Technikgestaltung der dort vorgelegte Operationalisierungsansatz zugrunde gelegt werden. Dabei kann an dieser Stelle davon ausgegangen werden, dass für die Entscheidung über den Referenzrahmen der der Anwendungsbereich des zu gestaltenden informationstechnischen Systems bereits festgelegt wurde.

Soweit als Grundlage dieser Entscheidung noch keine umfassende Akteursanalyse erstellt wurde, sind alle beteiligten oder zu beteiligenden Akteurinnen zu identifizieren und zu beschreiben, vor allem hinsichtlich ihrer Rollen sowie der individuellen, kollektiven und der gesellschaftlich geprägten oder konsentierten Erwartungen und Interessen. Anschließend sind die Zwecke zu identifizieren, die die Akteurinnen jeweils verfolgen.

Im Rahmen der Interessen-, Zweck- und Machtanalyse sind dann die Interessen und Zwecke vor dem Hintergrund, in welchem (Macht-)Verhältnis die Akteurinnen zueinander stehen und inwieweit sie voneinander abhängig sind, zueinander in Beziehung zu setzen und zu analysieren. Anschließend sind diese Interessen und Zwecke zu gewichten und zu bewerten, um darauf basierend zwischen den widerstreitenden Interessen und Zwecken abzuwägen. Abschließend sind die Zwecke, die das Informationssystem verfolgen soll, festzulegen.

Anschließend ist die anwendungsbereichsspezifische Bedrohungsanalyse durchzuführen und das Bedrohungsmodell zu generieren, das die Auswirkungen des Einsatzes des konkreten zu gestaltenden informationstechnischen Systems auf die Betroffenen und die Gesellschaft insgesamt darstellt. Dazu gehören die entstehenden Machtverschiebungen zwischen des Akteurinnen sowie die Folgen von zugrunde gelegten Modellannahmen und vorgesehenen Entscheidungsprogrammen, die dabei zugleich zu explizieren sind, aber auch die sich aus den einzelnen Verfahrenskomponenten in den einzelnen Verarbeitungsphasen ergebenden genauso wie die komponenten- und phasenübergreifenden besonderen Gefährdungen.

Für die identifizierten Bedrohungen sind dann angemessene Lösungen auszuwählen oder zu gestalten. Gestaltungsziele sind dabei die im vorherigen Kapitel ausführlich dargestellten Freiheits- und Partizipationsversprechen der modernen bürgerlichen Gesellschaft sowie die gesellschaftlichen Strukturschutzprinzipien und -mechanismen wie Gewaltenteilung, Machtbeschränkung, Transparenz oder Verfahrensgerechtigkeit.

Dabei wird grundsätzlich davon ausgegangen, dass es im Laufe dieses Prozesses erforderlich sein kann, zu einzelnen vorherigen Prozessschritten zurückzukehren, etwa um auf der Basis der Bedrohungsanalyse Ergänzungen oder Anpassungen an der Akteursdarstellung vorzunehmen oder um vor einer Übernahme von existierenden Lösungen in das eigene Entwicklungsprojekt dafür eine Bedrohungsanalyse zu erstellen. Auch erfordern Systemänderungen oder die Setzungen neuer Zwecke, aber auch wesentliche Änderungen im Anwendungsbereich, etwa durch das Auftreten neuer Akteurinnen in diesem Bereich, eine Wiederholung des Analyseprozesses.

Die zentralen Zwischenprodukte – die Anwendungsbereichsbestimmung, die Akteursanalyse sowie die Interessen-, Zweck- und Machtanalyse – sind für die Herstellung der Überprüfbarkeit des Bedrohungsmodells sowie der gewählten oder entwickelten Lösungen, etwa durch Aufsichtsorgane, Prüfinstitutionen oder Datenschutzvereinigungen, sowie als Grundlage für eine informierte Einwilligung von Betroffenen transparent zu machen. Die Veröffentlichung der Zwischenprodukte erzeugt zugleich eine starke Bindungswirkung, die mit einem an das Zweckbindungsprinzip angelehnten Modellbindungsprinzip noch verstärkt werden könnte.

5 Zusammenfassung und Abschluss

5.1 Zusammenfassung

In der historischen Systemanalyse der politischen und wissenschaftlichen Auseinandersetzungen zur Beschreibung, Einordnung und Begründung der Probleme, die mit den Begriffen *privacy*, Datenschutz und *surveillance* markiert werden, der jeweils vorgeschlagenen Lösungen oder Lösungsansätze, der Umsetzungen dieser Lösungen im Recht und ihrer Anwendung in der Praxis sowie der parallel geführten Debatten um eine zur Lösung des *privacy*-, Datenschutz- und *surveillance*-Problems geeignete und angemessene Technikgestaltung ist herausgearbeitet worden, dass es weder in der wissenschaftlichen noch in der politischen Debatte eine Einigung zu den unzähligen Aspekten gibt, die dieses Feld prägen. Die Unterschiede zwischen den Beschreibungen, Einordnungen und Erklärungen, die von den unterschiedlichen Beteiligten an dieser Debatte geliefert werden, sind stattdessen so groß und teilweise so grundlegend, so die Schlussfolgerung dieser Arbeit, dass die adressierten Phänomene, Praxen und Probleme als voneinander grundsätzlich verschieden verstanden werden müssen, auch wenn sie mit den gleichen Begriffen bezeichnet werden.

Diese Unterschiede fangen schon auf der Ebene des betrachteten Gegenstandsbereichs an. Sie betreffen die zugrunde gelegten Akteurskonstellationen – von interpersonalen Beziehungen über Beziehungen zwischen Individuen oder Gruppen und Organisationen bis zur gesellschaftlichen Informationsordnung insgesamt – sowie die Eigenschaften und Interessen der betrachteten Akteurinnen ebenso wie deren Umgang mit und Kontrolle über informationstechnische Systeme und die Zwecke, die sie damit verfolgen. Kurz: Die einzelnen Theorien oder Theorieschulen legen ihren Analysen teilweise überschneidungsfreie Phänomenbereiche zugrunde. Aber nicht nur hinsichtlich des Seins, sondern auch im Hinblick auf das Sollen, also die Zielvorstellungen oder Erwartungen, an denen sich das Informationsgebaren von Individuen, Gruppen und Organisationen, von Vereinen und Unternehmen, von Privaten und vom Staat oder von der Gesellschaft insgesamt messen lassen muss, gibt es einen tiefen Dissens. Die Menge der identifizierten Schutzgüter reicht dabei von individuellen Zuständen, Bedürfnissen, Interessen oder Werten über soziale Konstruktionen, gesellschaftliche Werte oder Normen bis hin zu Struktureigenschaften von gesellschaftlichen Verhältnissen, kann aber auch (fast) jede beliebige Kombination davon umfassen. Für die jeweils identifizierten Probleme – als Differenzen zwischen Sein und Sollen – und ihre Beschreibungen und Erklärungen folgt daraus, dass auch sie fundamental verschiedenen sind – und notwendig sein müssen. Dabei kann es sich um Artefakte wie Daten, Informationen oder Wissen handeln, um konkrete Handlungen oder Handlungsformen wie Überwachung, Missbrauch oder Informationsverarbeitung, um besondere Akteurskonstellationen oder deren Eigenschaften wie Machtimbalancen oder um gesellschaftliche Phänomene wie die Digitalisierung aller Lebensbereiche. Genauso umstritten sind die Beziehungen zwischen den Akteurinnen, Artefakten und Praxen und die jeweils daraus gezogenen Schlussfolgerungen für die Bestimmung, was Auslöser und was Folge ist, und was davon – Auslöser oder Folge – gerade das Problem bezeichnen soll und wie es einzuordnen und zu erklären ist. In der Folge werden wenig überraschend daher ganz unterschiedliche Lösungen oder Lösungsansätze vorgeschlagen: soziale Normen, rechtliche Rege-

lungen, der Markt oder technische Schutzsysteme, auch beliebig kombiniert und in verschiedenen konkreten Formen, die sich etwa danach bestimmen, wer oder was als Problem identifiziert wurde, wie das Problem charakterisiert und was als Auslöser identifiziert wurde. Auch ist deutlich geworden, dass es im Bereich der Diskussion um die Technikgestaltung an konsentierten oder auch nur durchgängig offengelegten Angreifer- und Bedrohungsmodellen mangelt.

Auch sind, wie die Analyse gezeigt hat, viele Konzepte, mit denen in der Debatte operiert wird, aus informatischer Sicht schlicht falsch, nicht, nicht mehr oder nicht vollumfänglich haltbar oder unzulässig verkürzt. Dazu gehören etwa die Fixierung auf personenbezogene Informationen sowohl hinsichtlich der Beschränkung des Gegenstandsbereichs als auch als Anknüpfungspunkt für Rechtssetzung und Technikgestaltung, die offenkundig falsche und doch weitverbreitete Behauptung, Sensitivität sei eine Eigenschaft von Informationen, die naive Trennung von „öffentlich“ und „privat“, das Konstrukt der informierten Einwilligung, vor allem in seiner derzeitigen Umsetzung, oder das sogenannte „Privacy Paradox“.

Darüber hinaus ist festzustellen, dass die Datenschutztheorie, deren Betrachtung im Zentrum der Arbeit stand, zumindest als Theorieschule gescheitert ist. Es ist dieser Schule nie gelungen, eine zugleich umfassende und dennoch lesbare Darstellung ihres Verständnisses vom Menschen und von der Welt, von Organisationen und von der Informationstechnik, von der Informationsverarbeitung und der Informationsgesellschaft vorzulegen, die die eigenen theoretischen Fundamente, Annahmen und Prämissen aufdeckt, das Datenschutzproblem auf dieser Basis fundiert erklärt und die vorgeschlagene Lösung – den Datenschutz – sauber begründet. Zwar hat sie die Entwicklung des deutschen – und damit vermittelt auch des europäischen Datenschutzrechts – wesentlich beeinflusst, sie hat jedoch zugelassen – oder sich sogar daran beteiligt –, dass das Datenschutzproblem von einem gesellschaftlichen Problem weitgehend auf eines der individuellen Entscheidung über die Preisgabe oder Nichtpreisgabe von personenbezogenen Informationen zurückgestutzt wurde. Und sie hat nicht verhindern können, dass aus der Datenschutzdiskussion, die immer zentral nur eine politische Diskussion sein kann, im Grunde eine reine Datenschutz*rechts*diskussion wurde, die damit nur noch zu den Bedingungen und gemäß den diskursiven Regeln der Rechtswissenschaft geführt werden kann.

Die vorliegende Arbeit hat es dann unternommen, den Datenschutz, den diese Theorieschule produziert hat, zu re-konstruieren. Dazu wurden die zugrunde gelegten Annahmen, der betrachtete Gegenstandsbereich, die auf dieser Basis durchgeführte Bedrohungsanalyse sowie die vorgeschlagene Lösungsarchitektur zur Abwehr der identifizierten Bedrohungen kompakt und zusammenhängend dargestellt und einer informatisch fundierten Kritik unterzogen. Dabei ist deutlich geworden, wie sehr die Datenschutztheorie von ihren Annahmen über Gesellschaft, Organisation und Technik sowie Technikgebrauch geprägt ist. Die Theorie geht von der Vorstellung einer modernen, funktional differenzierten Gesellschaft aus, die von Organisationen geprägt ist, bei denen es sich um rationale Bürokratien im Weberschen Sinne handelt. Diese Organisationen rationalisieren ihre Informationsverarbeitung zum Zwecke besserer Entscheidungsfindung und setzen dabei Computer als Werkzeuge ein, sowohl als Rationalisierungs- wie auch als Automatisierungswerkzeuge. Auf dieser Basis analysiert die Theorie, wie diese Praxen der Informationsverarbeitung und Entscheidungsfindung durch Organisationen mit den dafür eingesetzten Mitteln – Technik und Verfahren – überkommene gesellschaftliche Aushandlungsergebnisse – insbesondere in der konkreten Form, die sie im Recht gefunden haben – wie auch die Aushandlungsmechanismen selbst strukturell unterminieren. Als Kern des Datenschutzproblems werden dabei die strukturellen Machtimbalancen, die durch die Rationalisierung, Maschinisierung und Automation gesellschaftlicher Informationsverarbeitungsprozesse erzeugt, verstärkt oder verfestigt wer-

den, und deren Folgen für Individuen, Gruppen, Organisationen und die Gesellschaft insgesamt identifiziert. In der vorliegenden Arbeit wurde gezeigt, dass das verwendete Webersche Organisationsmodell für die Beschreibung und Analyse moderner Organisationen und ihrer Informationsverarbeitung und Entscheidungsfindung nicht mehr angemessen ist, dass dabei insbesondere die spezifische Rationalitätsunterstellung ein verzerrtes und damit unpassendes Bild moderner Organisationen und ihrer Informationspraxen erzeugt und dass die einseitige Charakterisierung von informationstechnischen Systemen als Werkzeuge gerade dafür blind ist, dass die Technik weder von organisationsinternen noch von organisationsexternen Akteurinnen ausschließlich instrumentell eingesetzt wird. Genauso mechanistisch wie das Webersche Organisationsmodell ist das Regelungsmodell, das die Datenschutztheorie vorgelegt hat, um die Informationsverarbeitungspraxen von Organisationen unter Bedingungen zu stellen. Insbesondere ist dabei die zugrunde gelegte Vorstellung der Erzeugbarkeit von Kontrollfähigkeit der Informationsverarbeitungprozesse tayloristisch, indem sie der Fehlannahme erliegt, dass die Zerlegung der Prozesse in Einzelschritte zugleich alle Probleme und Gefahren in Teilprobleme und Teilgefahren zerlegen könnte, die sich dann innerhalb der Einzelschritte abschließend bannen ließen. Bei allen aufgedeckten Einzelproblemen stellt die Arbeit aber auch fest, dass die Datenschutzdiskussion der 1970er Jahre für die Rationalisierung, Mechanisierung und Automation der Informationsverarbeitung und Entscheidungsfindung in Organisationen und deren gesellschaftliche Auswirkungen eine in Teilen sehr fundierte Analyse geliefert hat.

Die vorliegende Arbeit zieht daraus den Schluss, dass der Datenschutz als „Lösung“ des durch die Industrialisierung der gesellschaftlichen Informationsverarbeitung erzeugten Datenmachtproblems in der Informationsgesellschaft des 21. Jahrhunderts neu abgeleitet werden muss und dass dazu auf den von der historischen Datenschutztheorie vorgelegten Ableitungsprozess zurückgegriffen werden kann und sollte. Ausgangspunkt dieser Ableitung muss eine Analyse der gesellschaftlichen Informationsverarbeitung sein: Welche Eigenschaften haben die Akteurinnen – Organisationen, Individuen, Gruppen –, wie verarbeiten sie Informationen und treffen Entscheidungen, wie nutzen sie dabei welche Technik; schließlich: Wie „nutzt“ die Technik die Akteurinnen? Auf dieser Basis sind dann die Folgen dieser Informationsverarbeitungspraxen in vermachteten sozialen Beziehungen zu analysieren – und anschließend zu bewerten.

Eine solche Analyse legt die vorliegende Arbeit in Form eines dem Stand der wissenschaftlichen Debatte entsprechenden abstrakten – und damit jeweils noch anwendungsbereichsspezifisch zu konkretisierenden – Angreifermodells sowie eines analytischen Rasters für eine darauf aufbauende Bedrohungsanalyse vor. Diese Bedrohungsanalyse hat dabei das Problem der Machtverschiebung zwischen den Akteurinnen durch das zu gestaltende oder einzusetzende Verfahren sowie die sich aus den einzelnen Verfahrenskomponenten in den einzelnen Verarbeitungsphasen ergebenden genauso wie die komponenten- und phasenübergreifenden besonderen Gefährdungen anwendungsbereichsspezifisch zu konkretisieren und produziert dabei das Bedrohungsmodell, das dann als Grundlage für Auswahl und Gestaltung informationstechnischer Systeme dient. Dazu hat die vorliegende Arbeit einen prozeduralen Operationalisierungsansatz vorgelegt, der die Vorgehensweise und die jeweils zu analysierenden oder zu prüfenden inhaltlichen Fragen deutlich werden lässt. Dieses Vorgehensmodell ist dabei nicht nur für die Technikgestaltung nutzbar, sondern kann auch Basis eines prozeduralen Regelungsansatzes dienen. Zugleich zeigt die Arbeit, wie sich mit den Produkten der Akteursanalyse sowie der Interessen-, Zweck- und Machtanalyse eine pragmatische Lösung des Problems der informierten Einwilligung umsetzen lässt.

Anschließend wird das für die Technikgestaltung relevante Verhältnis zwischen dem rekonzeptionalisierten Datenschutz und dem geltenden – deutschen und europäischen – Datenschutzrecht

bestimmt, vor allem im Hinblick auf den jeweiligen Geltungsbereich, die verwendeten Informationsbegriffe und das jeweils zugrunde gelegte Prozessmodell der Informationsverarbeitung. Dabei wird deutlich, dass jedenfalls für Organisationen als Informationsverarbeiterinnen der Schutzbereich des Datenschutzes eine Obermenge des Schutzbereiches des Datenschutzrechts ist, womit grundsätzlich eine datenschutzfreundliche Informationsverarbeitung durch Organisationen auch als datenschutzrechtskonform gelten kann. Als defizitär wird besonders der Umgang des Rechts mit dem Informationsbegriff herausgestellt, dessen Potenziale, etwa bei Verwendung des der Datenschutztheorie zugrunde liegenden modelltheoretischen Informationsbegriffs, das Recht ungenutzt lässt, aber auch die Nichtnutzung des Phasenmodells, vor allem als Instrument für die Problemanalyse, aber auch – vor allem mit der neuen EU-Datenschutzgrundverordnung –, um an die einzelnen Phasen je spezifische rechtliche Anforderungen zu knüpfen.

Abschließend werden auf der Basis der gewonnenen Erkenntnisse Folgerungen für die Gestaltung datenschutzfreundlicher – und dabei nicht notwendig nur datenschutzrechtskonformer – informationstechnischer Systeme als Teilkomponenten von soziotechnischen Systemen gezogen.

Basierend auf der Feststellung, dass Datenschutzkonformität und Datenschutzrechtskonformität Eigenschaften von Informationsverarbeitungspraxen, nicht von Technik, sind, wird eine Klassifikation für die Charakterisierung von informationstechnischen Systemen hinsichtlich ihres Verhältnisses zu einem datenschutzkonformen Einsatz vorgelegt. Dabei wird zwischen (1) datenschutzfeindlichen Systemen, die gar nicht datenschutzkonform eingesetzt werden können, (2) datenschutzunfreundlichen, die einen datenschutzkonformen Einsatz behindern oder erschweren, (3) datenschutzneutralen, bei denen die Datenschutzkonformität nur von der Art und Weise des konkreten Einsatzes abhängt, (4) datenschutzfördernden, die einen datenschutzkonformen Einsatz unterstützen und einen nicht datenschutzkonformen erschweren, sowie (5) datenschutzgarantierenden Systemen, die unabhängig von der Intention der Datenverarbeiterin ausschließlich datenschutzkonform eingesetzt werden können, unterschieden. Vor dem Hintergrund von, vor allem im Bereich des Rechts vorgenommenen, Verantwortungszuschreibungen wird im Feld der datenschutzfördernden und datenschutzgarantierenden Systeme darüber hinaus zwischen (1) einfachen Unterstützungssystemen, (2) Systemen, die nicht unbewusst umgangen werden können, (3) Systemen, die weder unbewusst noch fahrlässig umgangen werden können, und (4) Systemen, die auch nicht vorsätzlich umgangen werden können, unterschieden. Anhand eines Beispiels wird mit Hilfe dieses Klassifikationsschemas gezeigt, wie Probleme im Bereich des Datenschutzes, die sich in keiner einzelnen der beteiligten Disziplinen lösen lassen, lösbar sind, wenn die Disziplinen kooperieren.

Als zentral für das Vorgehen bei der Auswahl zu verwendender und der Gestaltung neuer Technik hat die Arbeit die Entscheidung über den zu benutzenden Referenzrahmen identifiziert, also die Frage, welche *privacy-*, *surveillance-* oder Datenschutztheorie oder welches Recht als Bezugspunkt gelten soll. Damit entscheidet sich, welche Akteurinnen und Akteurskonstellationen, welche Zielvorstellungen und Schutzgüter und welche Probleme, Bedrohungen und Gefährdungen für diese Ziele und Schutzgüter in den Blick genommen werden können und zugleich, für welche dieser Probleme, Bedrohungen und Gefährdungen Lösungen gesucht oder entwickelt werden sollen. Während die Entscheidung für eine Theorie oder ein Recht vergleichsweise objektiv auf der Basis eines Vergleichs zwischen deren Geltungsbereichen und dem zukünftigen Anwendungsbereich der Technik getroffen werden kann, ist die Entscheidung über den Schutzbereich, wie die vorliegende Arbeit zeigt, immer eine immanent politische, keine rein wissenschaftliche. Nicht nur deshalb ist die Entscheidung über den zugrunde gelegten Referenzrahmen, wie alle anderen wesentlichen Entscheidungen auch, zu begründen und transparent zu machen. Aus

dem gewählten Referenzrahmen folgt, wie die Arbeit feststellt, in weiten Teilen das Vorgehen sowie die inhaltliche Ausgestaltung der einzelnen Schritte bei Bedrohungsanalyse und Technikgestaltung. Abschließend wird das am Beispiel des für den rekonzeptionalisierten Datenschutz vorgelegten Operationalisierungsansatz dargestellt.

5.2 Offene Forschungsfragen und mögliche Forschungsprogramme

Im Rahmen der vorliegenden Arbeit konnten nicht alle Fragen und Probleme, die sich im Zuge der Auseinandersetzung mit den Beschreibungen, Einordnungen und Begründungen verschiedener Theorien für die *privacy*-, Datenschutz- und *surveillance*-Probleme, den jeweils vorgeschlagenen Lösungen oder Lösungsansätzen, den Umsetzungen dieser Lösungen im Recht sowie der parallel geführten Debatten um eine zur Lösung der jeweiligen Probleme geeignete und angemessene Technikgestaltung ergaben, umfassend geklärt werden. Im Folgenden sollen daher diese offenen Forschungsfragen und möglichen Forschungsprogramme zumindest expliziert werden.

1. Es bedarf einer umfassenden Analyse und Gegenüberstellung der verschiedenen *privacy*-, Datenschutz- und *surveillance*-Theorien nach ihren Geltungsbereichen, ihren Annahmen über die Akteurinnen und deren Verhältnisse zueinander sowie ihren Schutzbereichen.

2. Für die existierenden Privacy-Enhancing Technologies sowie für die vorhandenen Systemkonzepte bedarf es einer Analyse der Frage, welche Probleme, Bedrohungen und Gefährdungen für welche Ziele und Schutzgüter sie jeweils in welchen Akteurskonstellationen zu lösen oder abzuwehren versuchen, also eines Mappings der Schutzbereiche auf die PETs.

3. Auf der anderen Seite ist für die verschiedenen Theorien und Gesetzesauslegungen jeweils zu untersuchen, welche Privacy-Enhancing Technologies und Konzeptvorschläge bereits existieren, die die jeweils identifizierten Probleme, Bedrohungen und Gefährdungen für Ziele und Schutzgüter in den betrachteten Akteurskonstellationen lösen oder abwehren können, also ein Mapping der PETs auf die Theorien.

4. Es bedarf einer Untersuchung, inwieweit sich der in dieser Arbeit rekonzeptionalisierte Datenschutz mit seinem systemanalytischen Ansatz und seinen Instrumenten über die hier dargestellten Ansätze hinaus für die Auslegung und Anwendung des überkommenen deutschen und europäischen Datenschutzrechts nutzbar machen lässt, vor allem für Datenschutz-Folgenabschätzungen, Datenschutz durch Technikgestaltung und Zertifizierungsverfahren nach der neuen EU-Datenschutzgrundverordnung.

5. Nachdem sich das Konzept der Schutzziele als interdisziplinär anschlussfähiges Instrument zur Konditionierung von Recht und Technik erfolgreich etabliert hat, sind die Schutzziele, die bislang nur aus dem überkommenen Datenschutzrecht abgeleitet wurden, neu aus dem in dieser Arbeit rekonzeptionalisierten Datenschutz abzuleiten, so dass sie sich nicht nur auf Verfahren mit den Komponenten Informationen, Prozesse und Systeme anwenden lassen, sondern auch auf die Organisationen selbst und deren Gestaltung.

6. Darüber hinaus sind die in Form von Schutzzielen formulierten materiellen Anforderungen phasenspezifisch zu konditionieren, mit möglicherweise jeweils unterschiedlichen führenden Schutzzielen.

Literaturverzeichnis

Abraham, Martin und Büschges, Günter: *Einführung in die Organisationssoziologie*. VS Verlag für Sozialwissenschaften, Wiesbaden, vierte Auflage, 2009.

Ackerman, Mark S., Cranor, Lorrie Faith und Reagle, Joseph, Jr.: Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In: *Proceedings of the 1st ACM Conference on Electronic Commerce*. ACM, 1999, S. 1–8.

Acquisti, Alessandro: Privacy in Electronic Commerce and the Economics of Immediate Gratification. In: *Proceedings of the 5th ACM conference on Electronic commerce*. ACM, 2004, S. 21–29.

Acquisti, Alessandro: Identity Management, Privacy, and Price Discrimination. In: *IEEE Security & Privacy*, Band 6(2): S. 46–50, 2008.

Acquisti, Alessandro und Grossklags, Jens: Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. In: *2nd Annual Workshop on Economics and Information Security (WEIS)*. 2003, Band 3, S. 1–27.

Acquisti, Alessandro und Grossklags, Jens: What Can Behavioral Economics Teach Us About Privacy? In: Acquisti, Alessandro, Gritzalis, Stefanos, Lambrinoudakis, Costas und De Capitani di Vimercati, Sabrina (Hg.) *Digital Privacy: Theory, Technologies and Practices*. Auerbach Publications, New York, London, 2007, S. 363–377.

Agre, Philip E.: The Architecture of Identity: Embedding privacy in market institutions. In: *Information, Communication & Society*, Band 2(1): S. 1–25, 1999.

Agre, Philip E.: P2P and the Promise of Internet Equality. In: *Communications of the ACM*, Band 46(2): S. 39–42, 2003.

Albers, Marion: Information als neue Dimension im Recht. In: *Rechtstheorie*, Band 33(1): S. 61–89, 2002.

Albers, Marion: *Informationelle Selbstbestimmung*. Nomos Verlagsgesellschaft, Baden-Baden, 2005.

Albers, Marion: Umgang mit personenbezogenen Informationen und Daten. In: Hoffmann-Riem, Wolfgang, Schmidt-Aßmann, Eberhard und Voßkuhle, Andreas (Hg.) *Grundlagen des Verwaltungsrechts, Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen*, C. H. Beck, Berlin, S. 107–220. 2008.

Allen, Anita L.: *Uneasy Access. Privacy for Women in a Free Society*. Rowman & Littlefield Publishers, Inc., Totowa, New Jersey, 1988.

Allen, Anita L.: *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Rowman & Littlefield, Lanham, 2003.

Allen, Anita L.: Natural Law, Slavery, and the Right to Privacy Tort. In: *Fordham Law Review*, Band 81(3): S. 1187–1216, 2012.

Allmer, Thomas: A critical contribution to theoretical foundations of privacy studies. In: *Journal of Information, Communication & Ethics in Society*, Band 9(2): S. 83–101, 2011.

Altman, Irwin: *The Environment and Social Behavior*. Brooks/Cole Publishing Company, Monterey, California, 1975.

Aly, Götz und Roth, Karl Heinz: *Die restlose Erfassung. Volkszählen, Identifizieren, Aussondern im Nationalsozialismus*. Rotbuch Verlag Berlin, Berlin, 1984.

Ambrose, Meg Leta: From the Avalanche of Numbers to Big Data: A Comparative Historical Perspective on Data Protection in Transition. In: O'Hara, Kieron, Nguyen, M-H. Carolyn und Haynes, Peter (Hg.) *Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment*, IOS Press, Berlin, S. 25–48. 2014.

Amesberger, Claus, Eidmann, Klaus, Heder, Peter, Marksteiner, Friedel und Schneider, Jochen: Datenschutz – Mittel und Maßnahmen für die Datenverarbeitung. Forschungsbericht DV 74-04, Siemens Aktiengesellschaft, 1974.

Anderson, James P.: Computer Security Technology Planning Study. Technical Report ESD-TR-73-51, U.S. Air Force Electronic Systems Division, 1972.

Anderson, Ross: The Eternity Service. In: *Pragocrypt'96*, S. 242–252, 1996.

Anderson, Ross: *Security Engineering: A Guide to Building Dependable Distributed Systems*, Band 2. John Wiley & Sons, New York, 2008.

Andersson, Christer, Camenisch, Jan, Crane, Stephen, Fischer-Hübner, Simone, Leenes, Ronald, Pearson, Siani, Pettersson, John Sören und Sommer, Dieter: Trust in PRIME. In: *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.* IEEE, 2005, S. 552–559.

Antón, Annie I.: Goal-Based Requirements Analysis. In: *Proceedings of the Second International Conference on Requirements Engineering*. IEEE, Colorado Springs, 1996, S. 136–144.

Antón, Annie I. und Earp, Julia B.: A Taxonomy for Web Site Privacy Requirements. Technical report, North Carolina State University, Raleigh, 2001.

Antón, Annie I. und Potts, Colin: ITR: Encoding Rights, Permissions and Obligations: Privacy Policy Specification and Compliance. 2003.

Anér, Kerstin: Attack is the best defence. In: *Management Informatics*, Band 1(5): S. 179–180, 1972.

Anér, Kerstin: Datengesetz und Datenschutz in Schweden. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975, S. 44–48.

Arbeitsgruppe „Datenschutzfreundliche Technologien" des Arbeitskreises „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzfreundliche Technologien. Arbeitspapier, 1997. Stand: 01.10.1997.

Ardagna, Claudio A., Camenisch, Jan, Kohlweiss, Markulf, Leenes, Ronald, Neven, Gregory, Priem, Bart, Samarati, Pierangela, Sommer, Dieter und Verdicchio, Mario: Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project. In: *Journal of Computer Security*, Band 18(1): S. 123–160, 2010.

Arnesen, Ragni Ryvold und Danielsson, Jerker: A Framework for Enforcement of Privacy Policies. In: *Proceedings of the Nordic Security Workshop NORDSEC*. 2003.

Arnesen, Ragni Ryvold, Danielsson, Jerker und Nordlund, Bjørn: Carnival: An Application Framework for Enforcement of Privacy Policies. In: *9th Nordic Workshop on Secure IT-systems*. 2004.

Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data. Working Paper WP 136, 2007.

Arvidsson, Adam: On the „Pre-History of The Panoptic Sort“: Mobility in Market Research. In: *Surveillance & Society*, Band 1(4): S. 456–474, 2002.

Ashley, Paul, Hada, Satoshi, Karjoth, Günter, Powers, Calvin und Schunter, Matthias: Enterprise Privacy Authorization Language (EPAL). Technischer Bericht, IBM Research, Rüschlikon, 2003.

Astin, Alexander W. und Boruch, Robert F.: A „Link“ System for Assuring Confidentiality of Research Data in Longitudinal Studies. In: Hoffman, Lance J. (Hg.) *Security and Privacy in Computer Systems*, Melville Publishing Company, Los Angeles, S. 294–303. 1973. Nachdruck aus: American Council on Education Research Report, Vol. 5, No. 3, Februar 1970.

Auernhammer, Herbert: Gedanken zur Datenschutzgesetzgebung. In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 1(0): S. 23–27, 1971.

Auernhammer, Herbert: Datenschutzgesetzgebung – Magna Charta des Bürgers von heute. In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation.* Deutsche Verlags-Anstalt, Stuttgart, 1975, S. 57–71.

Auernhammer, Herbert: Der neue Referentenentwurf zur Novellierung des Bundesdatenschutzgesetzes. In: *Datenschutz und Datensicherung*, Band 8(1): S. 5–10, 1984.

Austermühle, Gisa: *Zur Entstehung und Entwicklung eines persönlichen Geheimsphärenschutzes vom Spätabsolutismus bis zur Gesetzgebung des Deutschen Reiches.* Duncker & Humblot, Berlin, 2002.

Austin, Lisa M.: Enough About Me: Why Privacy is About Power, not Consent (or Harm). In: Sarat, Austin (Hg.) *A World without Privacy: What Law Can and Should Do?*, Cambridge University Press, Cambridge, S. 131–189. 2014.

Austin, Lisa M.: Surveillance and the Rule of Law. In: *Surveillance & Society*, Band 13(2): S. 295–299, 2015.

Backes, Michael, Karjoth, Günter, Bagga, Walid und Schunter, Matthias: Efficient Comparison of Enterprise Privacy Policies. In: *Proceedings of the 2004 ACM Symposium on Applied Computing.* ACM Press, New York, 2004, S. 375–382.

Baek, Young Min: Solving the privacy paradox: A counter-argument experimental approach. In: *Computers in Human Behavior*, Band 38: S. 33–42, 2014.

Bambauer, Jane, Muralidhar, Krishnamurty und Sarathy, Rathindra: Fool's Gold: An Illustrated Critique of Differential Privacy. Arizona Legal Studies Discussion Paper No. 13-47, James E. Rogers College of Law, The University of Arizona, 2013.

Baran, Paul: Communications, computers and people. In: *Proceedings of the November 30–December 1, 1965, fall joint computer conference, part II: computers: their impact on society.* ACM, New York, NY, USA, 1965, AFIPS '65 (Fall, part II), S. 45–49.

Baran, Paul: *On the Engineer's Responsibility in Protecting Privacy.* The RAND Corporation, Santa Monica, California, 1968.

Barnes, Susan B.: A privacy paradox: Social networking in the United States. In: *First Monday*, Band 11(9), 2006. URL `http://www.firstmonday.dk/ojs/index.php/fm/article/view/1394`.

Barocas, Solon und Selbst, Andrew D.: Big Data's Disparate Impact. In: *SSRN*, 2015. URL `https://ssrn.com/abstract=2477899`.

Barth, Adam, Datta, Anupam, Mitchell, John C. und Nissenbaum, Helen: Privacy and Contextual Integrity: Framework and Applications. In: *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. 2006.

Bateson, Gregory: *Steps to an Ecology of Mind. Collected Essays in Anthropology, Psychiatry, Evolution, and Epistemology*. Jason Aronson Inc., Northvale, 1987. Nachdruck. Ursprünglich veröffentlicht: San Franciso: Chandler Pub. Co., 1972.

Baum, Gerhart: Wacht auf, es geht um die Menschenwürde. In: *Datenschutz und Datensicherheit*, Band 37(9): S. 583–584, 2013.

Bayardo, Roberto J. und Agrawal, Rakesh: Data Privacy Through Optimal k-Anonymization. In: *Proceedings of the 21st International Conference on Data Engineering (ICDE 2005)*. IEEE, 2005, S. 217–228.

Beardsley, Elizabeth L.: Privacy: Autonomy and Selective Disclosure. In: Pennock, J. Roland und Chapman, John W. (Hg.) *Privacy*, Atherton Press, New York, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy*, S. 56–70. 1971.

Beckedahl, Markus und Meister, Andre (Hg.): *Überwachtes Netz : Edward Snowden und der größte Überwachungsskandal der Geschichte*. newthinking communications, Berlin, 2013.

Becker, Dirk: *Organisation als System*. Suhrkamp Verlag, 1999.

Beckers, Kristian: Comparing Privacy Requirements Engineering Approaches. In: *Seventh International Conference on Availability, Reliability and Security (ARES)*. IEEE, Prag, 2012, S. 574–581.

Behrendt, Heiko: Datenschutzaudit in der Realität. In: *Datenschutz und Datensicherheit*, Band 30(1): S. 20–23, 2006.

Belair, Robert R., Westin, Alan F. und Mullenholz, John J.: Privacy Implications Arising from Intelligent Vehicle-Highway Systems. techreport, prepared for the US Department of Transportation, Washington, DC, 1993.

Bellotti, Victoria und Sellen, Abigail: Design for Privacy in Ubiquitous Computing Environments. In: *Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work*. Kluwer Academic Publishers, Norwell, MA, 1993, ECSCW'93, Milan, Italy, S. 77–92.

Benda, Ernst: Privatsphäre und „Persönlichkeitsprofil". In: Leibholz, Gerhard, Faller, Hans Joachim, Mikat, Paul und Reis, Hans (Hg.) *Menschenwürde und freiheitliche Rechtsordnung. Festschrift für Willi Geiger zum 65. Geburtstag*, J. C. B. Mohr (Paul Siebeck), Tübingen, S. 23–44. 1974.

Benda, Ernst: Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz. In: *Datenschutz und Datensicherung*, Band 8(2): S. 86–90, 1984.

Beniger, James R.: *The Control Revolution. Technological and Economic Origins of the Information Society*. Harvard University Press, Cambridge, MA, 1986.

Benn, Stanley I.: Privacy, Freedom, and Respect for Persons. In: Pennock, J. Roland und Chapman, John W. (Hg.) *Privacy*, Atherton Press, New York, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy*, S. 1–26. 1971.

Bennett, Colin J.: Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States. In: *Governance*, Band 1(4): S. 415–441, 1988.

Bennett, Colin J.: Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s. In: *Science, Technology & Human Values*, Band 16(1): S. 51–69, 1991.

Bennett, Colin J.: *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press, Ithaca, NY, 1992.

Bennett, Colin J.: In Defence of Privacy: The concept and the regime. In: *Surveillance & Society*, Band 8(4): S. 485–496, 2011a.

Bennett, Colin J.: In further defence of privacy... In: *Surveillance & Society*, Band 8(4): S. 513–516, 2011b.

Bennett, Colin J. und Raab, Charles D.: *The Governance of Privacy: Policy instruments in a global perspective*. Ashgate, 2003.

Berghe, Chris Vanden und Schunter, Matthias: Privacy Injector — Automated Privacy Enforcement Through Aspects. In: Danezis, G. und Golle, E. (Hg.) *Privacy Enhancing Technologies (PET 2006)*. Springer, Berlin, Heidelberg, 2006, Band 4258 von *Lecture Notes in Computer Science*, S. 99–117.

Bergmann, Michael: Auf dem Weg zu einer rechtlichen Regelung des grenzüberschreitenden Datenflusses. In: Hohmann, Harald (Hg.) *Freiheitssicherung durch Datenschutz*. Suhrkamp Verlag, Frankfurt am Main, 1987, S. 205–218.

Bibas, Steven A.: A Contractual Approach to Data Privacy. In: *Harvard Journal of Law & Public Policy*, Band 17(2): S. 591–611, 1994.

Bieber, Horst: Die Diktatur der Daten: Sanft, aber wirkungsvoll verengt der Computer die Freiheit des Menschen. In: *Die Zeit*, 1978. 5. Mai.

Bigo, Didier, Carrera, Sergio, Hernanz, Nicholas, Jeandesboz, Julien, Parkin, Joanna, Ragazzi, Francesco und Scherrer, Amandine: Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law. 2013. Liberty and Security in Europe Papers 61.

Bing, Jon: Classification of Personal Information with Respect to the Sensitivity Aspect. In: *Data Banks and Society*, Universitetsforlaget, Oslo, S. 98–141. 1972.

Bing, Jon: Computers and Law: Some beginnings. In: *it-Information Technology (vormals it+ ti)*, Band 49(2): S. 71–82, 2007.

Birkelbach, Willi: Überlegungen nach dreijähriger Datenschutzpraxis. In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation*. Deutsche Verlags-Anstalt, Stuttgart, 1975, S. 10–27.

Birnhack, Michael D.: A Quest for a Theory of Privacy: Context and Control. In: *Jurimetrics*, Band 51(4): S. 447–479, 2011.

Birnhack, Michael D.: Reverse Engineering Informational Privacy Law. In: *Yale Journal of Law and Technology*, Band 15(1), 2013. Article 3, URL `http://digitalcommons.law.yale.edu/yjolt/vol15/iss1/3`.

Bischoff, Stefan: Zur Komplementierung des Datenschutzes unter organisatorischen Aspekten: Das Konzept der Zweckbindung. In: Traunmüller, Roland, Fiedler, Herbert, Grimmer, Klaus und Reinermann, Heinrich (Hg.) *Neue Informationstechnologien und Verwaltung*. Springer, Berlin, 1984, S. 193–211.

Bischoff, Stefan und Burkard, Benedikt: Zum Verhältnis von Datenschutz und Organisation. In: Kuhlen, Rainer (Hg.) *Koordination von Informationen*. Gesellschaft für Informatik, Springer, Berlin, Heidelberg, New York, 1984, Band 81 von *Informatik-Fachberichte*, S. 195–204.

Bizer, Johann: Technikfolgenabschätzung und Technikgestaltung im Datenschutzrecht. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 45–64. 1998.

Bizer, Johann: Datenschutz durch Technikgestaltung. In: Bäumler, Helmut und von Mutius, Albert (Hg.) *„Datenschutzgesetze der dritten Generation“: Texte und Materialien zur Modernisierung des Datenschutzrechts*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 28–59. 1999.

Bizer, Johann: Recht auf Anonymität – Ein Rechtsprinzip der elektronischen Individualkommunikation. In: Sokol, Bettina (Hg.) *Datenschutz und Anonymität*, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Düsseldorf, S. 59–71. 2000.

Bizer, Johann: Datenschutz in die Prozesse. In: *Datenschutz und Datensicherheit*, Band 30(10): S. 598–598, 2006a.

Bizer, Johann: Scoring: Ein Desaster der Kreditwirtschaft. In: *Datenschutz und Datensicherheit*, Band 30(7): S. 396–396, 2006b.

Bizer, Johann: Datenschutz als Gestaltungsaufgabe. In: *Datenschutz und Datensicherheit*, Band 31(10): S. 725–730, 2007a.

Bizer, Johann: Gateway: Datenschutz durch Prozessmanagement. In: *Datenschutz und Datensicherheit*, Band 31(4): S. 289, 2007b.

Bizer, Johann: Modernisierung des Datenschutzes: Vier Säulen des Datenschutzes. In: *Datenschutz und Datensicherheit*, Band 31(4): S. 264–266, 2007c.

Bizer, Johann, Dingel, Kai, Fabian, Benjamin, Günther, Oliver, Hansen, Markus, Klafft, Michael, Möller, Jan und Spiekermann, Sarah: TAUCIS: Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung. Studie im Auftrag des Bundesministeriums für Bildung und Forschung, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin (HU), 2006.

Bloch-Wehba, Hannah: Confronting Totalitarianism at Home: The Roots of European Privacy Protections. In: *Brooklyn Journal of International Law*, Band 40(3): S. 749, 2014.

Bloustein, Edward J.: Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. In: *New York University Law Review*, Band 39(4): S. 962–1007, 1964.

Bock, Kirsten: EuroPriSe – Präventiver Datenschutz. In: *Datenschutz und Datensicherheit*, Band 32(11): S. 712, 2008.

Bock, Kirsten: Instrumente des Datenschutzes und ihre Eignung in der Praxis – Zur Ungeeignetheit der Selbstregulierung im Datenschutzbereich. In: Pohle, Jörg und Knaut, Andrea (Hg.) *Fundationes I: Geschichte und Theorie des Datenschutzes*. Monsenstein und Vannerdat, Münster, 2014, S. 67–72.

Bock, Kirsten und Meissner, Sebastian: Datenschutz-Schutzziele im Recht. In: *Datenschutz und Datensicherheit*, Band 36(6): S. 425–431, 2012.

Bock, Kirsten und Rost, Martin: Privacy By Design und die Neuen Schutzziele. In: *Datenschutz und Datensicherheit*, Band 35(1): S. 30–35, 2011.

Boehm, Franziska: Assessing the New Instruments in EU–US Data Protection Law for Law Enforcement and Surveillance Purposes. In: *European Data Protection Law*, Band 2(2): S. 178–190, 2016.

Boneh, Dan, Feigenbaum, Joan, Silberschatz, Avi und Wright, Rebecca N.: Portia: Privacy, Obligations, and Rights in Technologies of Information Assessment. In: *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*, Band 27(1): S. 10–16, 2004.

Bonneau, Joseph und Preibusch, Sören: The Privacy Jungle: On the Market for Data Protection in Social Networks. In: Moore, Tyler, Pym, David und Ioannidis, Christos (Hg.) *Economics of Information Security and Privacy*. Springer, Berlin, 2010, S. 121–167.

Bonner, W. und Chiasson, M.: If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. In: *Information and Organization*, Band 15(4): S. 267–293, 2005.

Borking, John J.: Privacy Incorporated Software Agent (PISA): Proposal for Building a Privacy Guardian for the Electronic Age. In: Federrath, Hannes (Hg.) *Designing Privacy Enhancing Technologies*. Springer, 2001, Band 2009 von *Lecture Notes in Computer Science*, S. 130–140.

Borking, John J. und Raab, Charles D.: Laws, PETs and Other Technologies for Privacy Protection. In: *The Journal of Information, Law and Technology*, Band 1(1): S. 1–14, 2001.

boyd, danah und Crawford, Kate: Six Provocations for Big Data. In: *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. 2011.

Braman, Sandra: Privacy by design: Networked computing, 1969–1979. In: *new media & society*, Band 14(5): S. 798–814, 2011.

Brandimarte, Laura, Acquisti, Alessandro und Loewenstein, George: Misplaced Confidences: Privacy and the Control Paradox. In: *The Ninth Workshop on the Economics of Information Security (WEIS 2010)*. 2010.

Brandimarte, Laura, Acquisti, Alessandro und Loewenstein, George: Misplaced Confidences: Privacy and the Control Paradox. In: *Social Psychology and Personality Science*, Band 4(3): S. 340–347, 2013.

Braudel, Fernand: *The Mediterranean and the Mediterranean World in the Age of Philip II*, Band 1. Harper Collins, London, 1972.

Braudel, Fernand: *The Mediterranean and the Mediterranean World in the Age of Philip II*, Band 2. Harper Collins, London, 1973.

Breaux, Travis D. und Antón, Annie I.: Analyzing Goal Semantics for Rights, Permissions, and Obligations. In: *13th IEEE International Conference on Requirements Engineering, 2005. Proceedings.* IEEE, 2005, S. 177–186.

Breaux, Travis D. und Antón, Annie I.: Analyzing Regulatory Rules for Privacy and Security Requirements. Technical Report TR-2007-9, North Carolina State University, Raleigh, NC, 2007.

Breaux, Travis D., Vail, Matthew W. und Antón, Annie I.: Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations. In: *14th IEEE International Requirements Engineering Conference (RE'06)*. IEEE, 2006, S. 49–58.

Brennecke, Ralph: Kriterien zur Operationalisierung der faktischen Anonymisierung. In: Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros (Hg.) *Datenzugang und Datenschutz*, Athenäum, Königstein/Ts., S. 158–175. 1980.

Brenton, Myron: *The Privacy Invaders*. Coward-McCann, Inc., New York, 1964.

Brey, Philip: Freedom and privacy in ambient intelligence. In: *Ethics and Information Technology*, Band 7(3): S. 157–166, 2005.

Brinckmann, Hans: Datenschutz und Recht auf Information. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 77–89. 1973.

Brinckmann, Hans: Verwaltungsgliederung als Schranke von Planungs- und Informationsverbund. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 110–135. 1976.

Brinckmann, Hans: Vom Datenschutzrecht zum Recht des Verbraucher-, Arbeits- und Umweltschutzes. In: *Datenschutz und Datensicherung*, Band 6(3): S. 157–164, 1982.

Brinckmann, Hans, Grimmer, Klaus, Lenk, Klaus und Rave, Dieter: *Verwaltungsautomation. Thesen über Auswirkungen automatisierter Datenverarbeitung auf Binnenstruktur und Außenbeziehungen der öffentlichen Verwaltung.* S. Toeche-Mittler Verlag, Darmstadt, 1974.

Brinckmann, Hans und Kuhlmann, Stefan: *Computerbürokratie: Ergebnisse von 30 Jahren öffentlicher Verwaltung mit Informationstechnik.* Westdeutscher Verlag, Opladen, 1990.

Brink, Stefan: Kurzes Plädoyer für unser „Supergrundrecht“ auf informationelle Selbstbestimmung. In: *PinG*, Band 2(1): S. 15–17, 2014.

Britz, Gabriele: *Freie Entfaltung durch Selbstdarstellung: eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG.* Mohr Siebeck, Tübingen, 2007.

Brodie, Carolyn, Karat, Clare-Marie, Karat, John und Feng, Jinjuan: Usable Security and Privacy: A Case Study of Developing Privacy Management Tools. In: *Proceedings of the 2005 symposium on Usable privacy and security.* ACM, 2005, S. 35–43.

Brown, Barry: Studying the Internet Experience. Technical Report HPL-2001-49, HP Laboratories Bristol, Bristol, 2001.

Broy, Manfred, Cengarle, María Victoria und Geisberger, Eva: Cyber-Physical Systems: Imminent Challenges. In: Calinescu, Radu und Garlan, David (Hg.) *17th Monterey Workshop Large-Scale Complex IT Systems. Development, Operation and Management, Oxford, UK, March 19-21, 2012, Revised Selected Papers.* Springer, Berlin, 2012, S. 1–28.

Brunnstein, Klaus: Die Rolle der Informationstechnologie für die Gesellschaft. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger.* Peter Hammer Verlag, Wuppertal, 1975, S. 153–156.

Brunton, Finn und Nissenbaum, Helen: Vernacular resistance to data collection and analysis: A political theory of obfuscation. In: *First Monday*, Band 16(5), 2011. URL `http://www.firstmonday.dk/ojs/index.php/fm/article/view/3493`.

Bräunlich, Katharina, Richter, Philipp, Grimm, Rüdiger und Roßnagel, Alexander: Verbindung von CC-Schutzprofilen mit der Methode rechtlicher IT-Gestaltung KORA. In: *Datenschutz und Datensicherheit*, Band 35(2): S. 129–135, 2011.

Bräutigam, Lothar, Höller, Heinzpeter und Scholz, Renate: *Datenschutz als Anforderung an die Systemgestaltung*, Band 12 von *Sozialverträgliche Technikgestaltung.* Westdeutscher Verlag, Opladen, 1990.

Buchner, Benedikt: *Informationelle Selbstbestimmung im Privatrecht.* Mohr Siebeck, Tübingen, 2006.

Buchner, Benedikt: Die Einwilligung im Datenschutzrecht. In: *Datenschutz und Datensicherheit*, Band 34(1): S. 39–43, 2010.

Bull, Hans Peter: *Verwaltung durch Maschinen – Rechtsprobleme der Technisierung der Verwaltung.* G. Grote'sche Verlagsbuchhandlung KG, Köln, Berlin, zweite Auflage, 1964.

Bull, Hans Peter: Datenschutz als Informationsrecht und Gefahrenabwehr. In: *Neue Juristische Wochenschrift*, Band 32(23): S. 1177–1182, 1979.

Bull, Hans Peter: Verfassungsrechtlicher Datenschutz. In: Bieber, Roland und Nickel, Dietmar (Hg.) *Das Europa der zweiten Generation. Gedächtnisschrift für Christoph Sasse*, N. P. Engel Verlag, Kehl am Rhein, Band 2, S. 869–887. 1981a.

Bull, Hans Peter: *Ziele und Mittel des Datenschutzes.* Athenäum, Königstein/Taunus, 1981b.

Bull, Hans Peter: Informatik, Recht und Datenschutz. In: Kupka, Ingbert (Hg.) *GI – 13. Jahrestagung.* Gesellschaft für Informatik, Springer, Berlin, Heidelberg, New York, 1983, Band 73 von *Informatik-Fachberichte*, S. 21–23.

Bull, Hans Peter: *Datenschutz oder Die Angst vor dem Computer.* Piper, München, 1984.

Bull, Hans Peter: Vom Datenschutz zum Informationsrecht – Hoffnungen und Enttäuschungen. In: Hohmann, Harald (Hg.) *Freiheitssicherung durch Datenschutz.* Suhrkamp Verlag, Frankfurt am Main, 1987, S. 173–204.

Bull, Hans Peter: Mehr Datenschutz durch weniger Verrechtlichung – Zur Überarbeitung von Form und Inhalt der Datenschutzvorschriften. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 25–34. 1998a.

Bull, Hans Peter: Neue Konzepte, neue Instrumente? In: *Zeitschrift für Rechtspolitik*, Band 31(8): S. 310–314, 1998b.

Bull, Hans Peter: Reasonable Expectations of Privacy. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 85–99. 2004.

Bull, Hans Peter: Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese. In: *Neue Juristische Wochenschrift*, S. 1617–1624, 2006.

Bull, Hans Peter: *Informationelle Selbstbestimmung – Vision oder Illusion?* Mohr Siebeck, Tübingen, 2009.

Bull, Hans Peter: *Netzpolitik: Freiheit und Rechtsschutz im Internet.* Nomos Verlagsgesellschaft, Baden-Baden, 2013.

Bundesministerium des Innern: Das Volkszählungsgesetz-Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 – 1 BvR 209/83 u. a. – Erste Folgerungen. Vorlage des Bundesministers des Innern an den Innenausschuß des Deutschen Bundestages vom 25. April 1984. In: *Datenschutz und Datensicherung*, Band 8(4): S. 281–289, 1984.

Burgoon, Judee K.: Privacy and Communication. In: *Annals of the International Communication Association*, Band 6(1): S. 206–249, 1982.

Burk, Holger und Pfitzmann, Andreas: Digital Payment Systems Enabling Security and Unobservability. In: *Computers & Security*, Band 8(5): S. 399–416, 1989.

Burkert, Herbert: Das Problem des Zusatzwissens. In: Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros (Hg.) *Datenzugang und Datenschutz*, Athenäum, Königstein/Ts., S. 143–147. 1980.

Burkert, Herbert: Einige Anmerkungen zur rechtlichen Gestaltung der Kommunikationsbeziehungen Bürger/öffentliche Verwaltung unter Berücksichtigung neuer Kommunikationstechniken insbesondere Bildschirmtext. In: Traunmüller, Roland, Fiedler, Herbert, Grimmer, Klaus und Reinermann, Heinrich (Hg.) *Neue Informationstechnologien und Verwaltung.* Springer, 1984, Band 80 von *Informatik-Fachberichte*, S. 183–192.

Burkert, Herbert: *Datenschutz und Informations- und Kommunikationstechnik. Eine Problemskizze.* Nummer 6 in Werkstattbericht. Ministerium für Arbeit, Gesundheit und Soziales des Landes NRW, Düsseldorf, 1985.

Burkert, Herbert: Privacy-enhancing technologies: typology, critique, vision. In: Agre, Philip E. und Rotenberg, Marc (Hg.) *Technology and privacy: the new landscape*, MIT Press, Cambridge, MA, USA, S. 125–142. 1997.

BVerfG: KPD-Verbot. BVerfGE 5, 85, 1956.

BVerfG: Elfes. BVerfGE 6, 32, 1957.

BVerfG: Mikrozensus. BVerfGE 27, 1, 1969.

BVerfG: Ehescheidungsakten. BVerfGE 27, 344, 1970.

BVerfG: Volkszählung. BVerfGE 65, 1, 1983.

BVerfG: Tagebuchaufzeichnungen. BVerfGE 80, 367, 1989.

BVerfG: Offenbarung der Entmündigung. BVerfGE 84, 192, 1991.

BVerfG: Kontostammdaten. BVerfGE 118, 164, 2007.

BVerfG: Online-Durchsuchungen. BVerfGE 120, 274, 2008.

Bygrave, Lee A.: International agreements to protect personal data. In: Rule, James B. und Greenleaf, Graham (Hg.) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, S. 15–49. 2008.

Bäumler, Helmut: Normenklarheit als Instrument der Transparenz. In: *Juristische Rundschau*, Band 1984(9): S. 361–366, 1984.

Bäumler, Helmut: Das Recht auf informationelle Selbstbestimmung im Sicherheitsbereich und der maschinenlesbare Ausweis. In: Hohmann, Harald (Hg.) *Freiheitssicherung durch Datenschutz*. Suhrkamp Verlag, Frankfurt am Main, 1987, S. 235–260.

Bäumler, Helmut und von Mutius, Albert (Hg.): *Datenschutz als Wettbewerbsvorteil. Privacy sells: Mit modernen Datenschutzkomponenten Erfolg beim Kunden*. Vieweg, Braunschweig / Wiesbaden, 2002.

Bölsche, Jochen: *Der Weg in den Überwachungsstaat*. Rowohlt, Reinbek bei Hamburg, 1979.

Bühnemann, Bernt: Datenschutz im privatwirtschaftlichen Bereich. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 91–106. 1973.

Bühnemann, Bernt: *Datenschutz im nicht-öffentlichen Bereich*. Beiheft 4, Datenverarbeitung im Recht (DVR). J. Schweitzer Verlag, Berlin, 1974.

Büllesbach, Alfred: *Informationstechnologie und Datenschutz*. J. Schweitzer Verlag, München, 1985.

Büllesbach, Alfred: Die Kunst der Selbstregulierung. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 239–252. 2004.

Büllesbach, Alfred und Garstka, Hans-Jürgen: Meilensteine auf dem Weg zu einer datenschutzgerechten Gesellschaft. In: *Computer & Recht*, Band 21(10): S. 720–724, 2005.

Camenisch, Jan, Leenes, Ronald, Hansen, Marit und Schallaböck, Jan: An Introduction to Privacy-Enhancing Identity Management. In: Camenisch, Jan, Leenes, Ronald und Sommer, Dieter (Hg.) *Digital Privacy*. Springer, Berlin, Heidelberg, 2011, Band 6545 von *Lecture Notes in Computer Science*, S. 3–21.

Camenisch, Jan, Sommer, Dieter, Fischer-Hübner, Simone, Hansen, Marit, Krasemann, Henry, Lacoste, Gérard, Leenes, Ronald, Tseng, Jimmy und shelat, abhi: Privacy and Identity Management for Everyone. In: *Proceedings of the 2005 workshop on Digital Identity Management*. ACM, 2005, S. 20–27.

Campbell, Duncan: Inside Echelon. In: Schulzki-Haddouti, Christiane (Hg.) *Vom Ende der Anonymität: Die Globalisierung der Überwachung*, Verlag Heinz Heise, Hannover, S. 49–70. 2000.

Caplan, Robyn und boyd, danah: Who Controls the Public Sphere in an Era of Algorithms? – Mediation, Automation, Power. In: *Who Controls the Public Sphere in an Era of Algorithms?* Data & Society, 2016. URL `http://www.datasociety.net/pubs/ap/MediationAutomationPower_2016.pdf`.

Capurro, Rafael, Eldred, Michael und Nagel, Daniel: *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld*. ontos verlag, Frankfurt am Main, 2013.

Carolan, Eoin und Castillo-Mayen, M. Rosario: Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws. In: *Virginia Journal of Law & Technology*, Band 19(2): S. 324–387, 2014.

Casassa Mont, Mario: On Privacy-aware Information Lifecycle Management in Enterprises: Setting the Context. Technical Report HPL-2006-109, Trusted Systems Laboratory, HP Laboratories, Bristol, 2006a.

Casassa Mont, Mario: Towards Scalable Management of Privacy Obligations in Enterprises. In: Fischer-Hübner, Simone (Hg.) *TrustBus 2006*. Springer, Berlin, Heidelberg, 2006b, Band 4083 von *Lecture Notes in Computer Science*, S. 1–10.

Cate, Fred H.: The Privacy Paradox. In: *76th Annual Winter Newspaper Institute*. North Carolina Press Association, Chapel Hill, NC, 2001.

Cate, Fred H.: The Failure of Fair Information Practice Principles. In: Winn, Jane K. (Hg.) *Consumer Protection in the Age of the Information Economy*, Ashgate, Aldershot, Kapitel 13, S. 343–379. 2006.

Cate, Fred H., Cullen, Peter und Mayer-Schönberger, Viktor: *Data Protection Principles for the 21st Century*. Microsoft Corporaton, 2013. URL `http://www.repository.law.indiana.edu/facbooks/23`.

Catlett, Jason: Privacy, Property and P3P: A Critique of Lessig's Code. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 185–188. 2000.

Cavoukian, Ann: Privacy Design Principles for an Integrated Justice System. Working paper, Information and Privacy Commissioner of Ontario, Toronto, Ontario, 2000.

Cavoukian, Ann: Privacy by Design: The 7 Foundational Principles. 2010. Revised: Oktober 2010.

Cavoukian, Ann, Taylor, Scott und Abrams, Martin E.: Privacy by Design: essential for organizational accountability and strong business practices. In: *Identity in the Information Society*, Band 3(2): S. 405–413, 2010.

Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: *Communications of the ACM*, Band 24(2): S. 84–90, 1981. doi:10.1145/358549.358563.

Chaum, David: Blind Signatures for Untraceable Payments. In: Chaum, David, Rivest, Ronald L. und Sherman, Alan T. (Hg.) *Advances in Cryptology: Proceedings of Crypto 82*. Springer, Boston, MA, 1983, S. 199–203.

Chaum, David: A New Paradigm for Individuals in the Information Age. In: *IEEE Security & Privacy*, S. 99–103, 1984.

Chaum, David: New Secret Codes can Prevent a Computerized Big Brother. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 33–34. 1985a.

Chaum, David: New Secret Codes Can Prevent a Computerized Big Brother. In: Blakley, George und Chaum, David (Hg.) *Advances in Cryptology*, Springer, Berlin / Heidelberg, Band 196 von *Lecture Notes in Computer Science*, S. 432–433. 1985b.

Chaum, David: Security without identification: Transaction systems to make big brother obsolete. In: *Communications of the ACM*, Band 28(10): S. 1030–1044, 1985c. doi:10.1145/4372.4373.

Citron, Danielle Keats: Technological Due Process. In: *Washington University Law Review*, Band 85(6): S. 1249–1313, 2008.

Citron, Danielle Keats und Pasquale, Frank: The Scored Society: Due Process for Automated Predictions. In: *Washington Law Review*, Band 89(1): S. 1–33, 2014.

Clarke, Ian, Sandberg, Oskar, Wiley, Brandon und Hong, Theodore W.: Freenet: A Distributed Anonymous Information Storage and Retrieval System. In: Federrath, Hannes (Hg.) *Designing Privacy Enhancing Technologies*. Springer, 2001, Band 2009 von *Lecture Notes in Computer Science*, S. 46–66.

Clarke, Roger A.: Information technology and dataveillance. In: *Communications of the ACM*, Band 31(5): S. 498–512, 1988. doi:10.1145/42411.42413.

Clarke, Roger A.: Profiling: A hidden challenge to the regulation of data surveillance. In: *Journal of Law and Information Science*, Band 4(2): S. 403, 1993.

Clarke, Roger A.: The digital persona and its application to data surveillance. In: *The Information Society*, Band 10(2): S. 77–92, 1994.

Clarke, Roger A.: *Data Surveillance: Theory, Practice & Policy*. Dissertation, Australian National University, Canberra, 1995. URL `http://www.rogerclarke.com/DV/PhD.html`.

Clarke, Roger A.: The Platform for Privacy Preferences: A critique. In: *Privacy Law and Policy Reporter*, Band 5(3): S. 46–48, 1998a.

Clarke, Roger A.: The Platform for Privacy Preferences: An overview. In: *Privacy Law and Policy Reporter*, Band 5(2): S. 35–39, 1998b.

Clarke, Roger A.: Privacy Impact Assessment. 1999. URL `http://www.rogerclarke.com/DV/PIA.html`.

Clarke, Roger A.: Meta-brands: privacy marks and seals. In: *Privacy Law and Policy Reporter*, 2001.

Clarke, Roger A.: Privacy impact assessment: Its origins and development. In: *Computer Law & Security Review*, Band 25: S. 123–135, 2009.

Clauß, Sebastian, Kesdogan, Dogan und Kölsch, Tobias: Privacy Enhancing Identity Management: Protection Against Re-identification and Profiling. In: *Proceedings of the 2005 Workshop on Digital Identity Management*. ACM, New York, NY, USA, 2005, S. 84–93.

Clement, Andrew: Considering Privacy in the Development of Multi-media Communications. In: *Computer Supported Cooperative Work (CSCW)*, Band 2(1): S. 67–88, 1994.

Cohen, Julie E.: Examined Lives: Informational Privacy and the Subject as Object. In: *Stanford Law Review*, Band 52: S. 1373–1438, 2000a.

Cohen, Julie E.: Privacy, Ideology, and Technology: A Response to Jeffrey Rosen. In: *Georgetown Law Journal*, Band 89: S. 2029–2045, 2000b.

Cohen, Julie E.: Privacy, Visibility, Transparency, and Exposure. In: *University of Chicago Law Review*, Band 75: S. 181–201, 2008.

Cohen, Julie E.: What Privacy Is For. In: *Harvard Law Review*, Band 126: S. 1904–1933, 2013.

Cohen, Julie E.: The Surveillance-Innovation Complex: The Irony of the Participatory Turn. In: *SSRN*, 2014. URL `https://ssrn.com/abstract=2466708`.

Colesky, Michael, Hoepman, Jaap-Henk und Hillen, Christiaan: A Critical Analysis of Privacy Design Strategies. In: *2016 IEEE Security and Privacy Workshops (SPW)*. 2016, S. 33–40. doi:10.1109/SPW.2016.23.

Coll, Sami: Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance. In: *Information, Communication & Society*, Band 17(10): S. 1250–1263, 2014.

Compagna, Luca, El Khoury, Paul, Krausová, Alzbeta, Massacci, Fabio und Zannone, Nicola: How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. In: *Artificial Intelligence and Law*, Band 17(1): S. 1–30, 2009.

Compagna, Luca, El Khoury, Paul, Massacci, Fabio, Thomas, Reshma und Zannone, Nicola: How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach. In: *Proceedings of the 11th international conference on Artificial intelligence and law*. ACM, 2007, S. 149–153.

Conklin, Kenneth R.: Privacy: Should There Be A Right To It? In: *Educational Theory*, Band 26(3): S. 263–270, 1976.

Connolly, Chris, Greenleaf, Graham und Waters, Nigel: Privacy Self-Regulation in Crisis? – TRUSTe's 'Deceptive' Practices. In: *Privacy Laws & Business International Report*, (132): S. 13–17, 2014.

Council of Economic Advisers: Big Data and Differential Pricing. Report, Executive Office of the President of the United States, 2015.

Cox, Lawrence H.: Suppression Methodology and Statistical Disclosure Control. Confidentiality in Surveys. Report Nr. 26, Department of Statistics, University of Stockholm, Stockholm, 1978.

Cox, Lawrence H.: Disclosure Avoidance Practices For Releasing Microdata. In: Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros (Hg.) *Datenzugang und Datenschutz*, Athenäum, Königstein/Ts., S. 148–157. 1980.

Coy, Wolfgang: Für eine Theorie der Informatik! In: Coy, Wolfgang et al. (Hg.) *Sichtweisen der Informatik*, Vieweg, Braunschweig/Wiesbaden, S. 17–32. 1992.

Coy, Wolfgang: Weder vollständig noch widerspruchsfrei. In: Bizer, Johann, Lutterbeck, Bernd und Rieß, Joachim (Hg.) *Umbruch von Regelungssystemen in der Informationsgesellschaft. Freundesgabe für Alfred Büllesbach*, S. 87–92. 2002.

Coy, Wolfgang: „Wenn ich einen würdigen Nachfolger gehabt hätte…" – Wilhelm Steinmüllers Zeit als Professor für Angewandte Informatik an der Universität Bremen. In: Garstka, Hansjürgen und Coy, Wolfgang (Hg.) *Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis*. Humboldt-Universität zu Berlin, Hermann von Helmholtz-Zentrum für Kulturtechnik, Berlin, 2014, S. 89–102.

Cranor, Lorrie Faith: Agents of choice: Tools that facilitate notice and choice about web site data practices. In: *arXiv preprint cs/0001011*, 2000a.

Cranor, Lorrie Faith: Privacy Tools. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 107–119. 2000b.

Cranor, Lorrie Faith und Reagle, Joseph, Jr.: Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project. In: MacKie-Mason, Jeffrey K. und Waterman, David (Hg.) *Telephony, the Internet, and the Media: Selected Papers from the 1997 Telecommunications Policy Research Conference*. Lawrence Erlbaum Associates, Mahwah, New Jersey, 1998, S. 215–232.

Cranor, Lorrie Faith, Reagle, Joseph, Jr. und Ackerman, Mark S.: Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. Technical Report TR 99.4.3, AT&T Labs-Research, Florham Park, NJ, 1999. URL `http://arxiv.org/html/cs/9904010v1/report.htm`.

Crawford, Kate und Schultz, Jason: Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. In: *Boston College Law Review*, Band 55(1): S. 93–128, 2014.

Culnan, Mary J.: Protecting Privacy Online: Is Self-Regulation Working? In: *Journal of Public Policy & Marketing*, Band 19(1): S. 20–26, 2000.

Custers, Bart, van der Hof, Simone, Schermer, Bart, Appleby-Arnold, Sandra und Brockdorff, Noellie: Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law. In: *SCRIPTed*, Band 10(4): S. 435–457, 2013.

D'Acquisto, Giuseppe, Domingo-Ferrer, Josep, Kikiras, Panayiotis, Torra, Vicenç, de Montjoye, Yves-Alexandre und Bourka, Athena: Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. Report, ENISA, 2015.

Dahrendorf, Ralf: *Homo Sociologicus. Ein Versuch zur Geschichte, Bedeutung und Kritik der Kategorie der sozialen Rolle*. Westdeutscher Verlag, Köln, Opladen, fünfte Auflage, 1965.

Dalenius, Tore: Towards a methodology for statistical disclosure control. In: *Statistik Tidskrift*, Band 15: S. 429–444, 1977.

Dammann, Ulrich: Datenschutzprobleme bei Planungs- und Entscheidungshilfesystemen. Dargestellt am Beispiel des HEPAS. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 257–278. 1973.

Dammann, Ulrich: Der Bürger in der Datenbank. In: Dammann, Ulrich, Karhausen, Mark O., Müller, Paul J. und Steinmüller, Wilhelm (Hg.) *Datenbanken und Datenschutz*, Herder & Herder, Frankfurt am Main, S. 1–49. 1974a.

Dammann, Ulrich: Strukturwandel der Information und Datenschutz. In: *Datenverarbeitung im Recht*, Band 3(3/4): S. 267–301, 1974b.

Dammann, Ulrich: Zur politischen Kontrolle von Planungsinformationssystemen. In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation.* Deutsche Verlags-Anstalt, Stuttgart, 1975, S. 105–117.

Dammann, Ulrich: Datenschutzkontrolle. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 50–69. 1976a.

Dammann, Ulrich: Manipulation oder Öffentlichkeitsinformation? Zur Funktion von Planungsinformationssystemen. In: Lenk, Klaus (Hg.) *Informationsrechte und Kommunikationspolitik*. S. Toeche-Mittler Verlag, Darmstadt, 1976b, Band 4 von *Beiträge zur juristischen Informatik*, S. 137–163.

Dammann, Ulrich, Karhausen, Mark O., Müller, Paul J. und Steinmüller, Wilhelm (Hg.): *Datenbanken und Datenschutz*. Herder & Herder, Frankfurt am Main, 1974.

Danezis, George, Domingo-Ferrer, Josep, Hansen, Marit, Hoepman, Jaap-Henk, Le Métayer, Daniel, Tirtea, Rodica und Schiffner, Stefan: Privacy and Data Protection by Design – from policy to engineering. Report, ENISA, 2014.

Danezis, George und Gürses, Seda: A critical review of 10 years of Privacy Technology. In: *Proceedings of Surveillance Cultures: A Global Surveillance Society?* 2010.

Dardenne, Anne, van Lamsweerde, Axel und Fickas, Stephen: Goal-directed requirements acquisition. In: *Science of computer programming*, Band 20(1-2): S. 3–50, 1993.

Datenschutzkommission des Deutschen Juristentages: *Grundsätze für eine Regelung des Datenschutzes*. C. H. Beck'sche Verlagsbuchhandlung, München, 1974.

De Hert, Paul und Gutwirth, Serge: Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. In: Claes, Erik, Duff, Antony und Gutwirth, Serge (Hg.) *Privacy and the Criminal Law*. Intersentia, Antwerpen, Oxford, 2006, S. 61–104.

De Hert, Paul und Papakonstantinou, Vagelis: The new General Data Protection Regulation: Still a sound system for the protection of individuals? In: *Computer Law & Security Review*, Band 32(2): S. 179–194, 2016.

DeCew, Judith Wagner: *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, 1997.

DeDeo, Simon: Wrong side of the tracks: Big Data and Protected Categories. In: *arXiv preprint arXiv:1412.4643v2*, 2015.

Denninger, Erhard: Das Recht auf informationelle Selbstbestimmung und Innere Sicherheit. In: *Kritische Justiz*, S. 215–244, 1985.

Denninger, Erhard: Das Recht auf informationelle Selbstbestimmung. In: Hohmann, Harald (Hg.) *Freiheitssicherung durch Datenschutz*. Suhrkamp Verlag, Frankfurt am Main, 1987, S. 127–172.

Der Bundesbeauftragte für den Datenschutz: Thesen zur Novellierung des Bundesdatenschutzgesetzes. In: *Datenschutz und Datensicherung*, Band 5(4): S. 223, 1981.

Dette, Klaus: Einführung in das Kolloquium und Zusammenfassung der Ergebnisse. In: Dette, Klaus, Kreibich, Rolf und Steinmüller, Wilhelm (Hg.) *Zweiweg-Kabelfernsehen und Datenschutz*. Institut für Zukunftsforschung, Minerva Publikation, München, 1979, Band 1 von *Beiträge des Instituts für Zukunftsforschung*, S. 3–13. Dokumentation des Colloquiums vom 12. September 1978 „Zweiweg-Kabelfernsehen und Datenschutz".

Dette, Klaus, Kreibich, Rolf und Steinmüller, Wilhelm (Hg.): *Zweiweg-Kabelfernsehen und Datenschutz*, Band 1 von *Beiträge des Instituts für Zukunftsforschung*. Minerva Publikation, München, 1979. Dokumentation des Colloquiums vom 12. September 1978 „Zweiweg-Kabelfernsehen und Datenschutz".

Deutsche Vereinigung für Datenschutz: DuD Report: 10 Jahre Volkszählungsurteil aus Sicht der DVD. In: *Datenschutz und Datensicherheit*, Band 18(2): S. 109–114, 1994.

Dienlin, Tobias und Trepte, Sabine: Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. In: *European Journal of Social Psychology*, Band 45(3): S. 285–297, 2015.

Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.): *Datenschutz und Datensicherung*. J. P. Bachem Verlag, Köln, 1976. Referate der gemeinsamen Fachtagung der Österreichischen Gesellschaft für Informatik (ÖGI) und der Gesellschaft für Informatik (GI), Johannes-Kepler-Universität, Linz, Österreich, 21. bis 23 September 1976.

Diffie, Whitfield und Landau, Susan: *Privacy on the Line – The Politics of Wiretapping and Encryption.* The MIT Press, Cambridge, Massachusetts, 1998.

Dingledine, Roger, Freedman, Michael J. und Molnar, David: The Free Haven Project: Distributed Anonymous Storage Service. In: Federrath, Hannes (Hg.) *Designing Privacy Enhancing Technologies.* Springer, 2001, Band 2009 von *Lecture Notes in Computer Science*, S. 67–95.

Dippoldsmann, Peter, Genrich, Helga und Poetsch, Jochen: Datenschutz als Kriterium für angepasste Informationstechnik. In: Kupka, Ingbert (Hg.) *GI – 13. Jahrestagung.* Gesellschaft für Informatik, Springer, Berlin, Heidelberg, New York, 1983, Band 73 von *Informatik-Fachberichte*, S. 419–427.

Dix, Alexander: Internationale Aspekte. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 93–106. 2000.

Dix, Alexander: Modernisierung des Datenschutzes: Lösungsansätze. In: *Datenschutz und Datensicherheit*, Band 31(4): S. 256–258, 2007.

Domingo-Ferrer, Josep und Soria-Comas, Jordi: From t-closeness to differential privacy and vice versa in data anonymization. In: *Knowledge-Based Systems*, Band 74: S. 151–158, 2015.

Domingo-Ferrer, Josep und Torra, Vicenc: A Critique of k-Anonymity and Some of Its Enhancements. In: *Third International Conference on Availability, Reliability and Security (ARES 08)*. IEEE, 2008, S. 990–993.

Donos, Pelopidas Konstantinos: *Datenschutz – Prinzipien und Ziele*, Band 11 von *Frankfurter Studien zum Datenschutz.* Nomos Verlagsgesellschaft, Baden-Baden, 1998.

Drackert, Stefan: *Die Risiken der Verarbeitung personenbezogener Daten.* Nummer S 149 in Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Duncker & Humblot, Berlin, 2014.

Drepper, Thomas: *Organisationen der GeselIschaft: Gesellschaft und Organisation in der Systemtheorie Niklas Luhmanns.* Westdeutscher Verlag, Wiesbaden, 2003.

Dunn, Edgar S.: The Idea of a National Data Center and the Issue of Personal Privacy. In: *The American Statistician*, Band 21(1): S. 21–27, 1967.

Duttge, Gunnar: Die Hypertrophie des Datenschutzes. In: *Humboldt Forum Recht*, Band 3(4): S. 29–41, 1998.

Dwork, Cynthia: Differential Privacy. In: *Automata, languages and programming (ICALP 2006). Part II.* Springer, Berlin, Heidelberg, 2006, Band 4052 von *Lecture Notes in Computer Science*, S. 1–12.

Dwork, Cynthia und Mulligan, Deidre K.: It's Not Privacy, and It's Not Fair. In: *Stanford Law Review Online*, Band 66: S. 35–40, 2013.

Däubler, Wolfgang, Klebe, Thomas, Wedde, Thomas und Weichert, Thilo (Hg.): *Bundesdatenschutzgesetz – Kompaktkommentar zu BDSG.* Bund-Verlag GmbH, dritte Auflage, 2010.

Earp, Julia B., Antón, Annie I. und Jarvinen, Olli: A Social, Technical and Legal Framework for Privacy Management and Policies. In: *Americas Conference on Information Systems (AMCIS)*. 2002, S. 605–612.

Eckhardt, Jens: BDSG: Neuregelungen seit 01.09.2009. In: *Datenschutz und Datensicherheit*, Band 33(10): S. 587–595, 2009.

Eckhardt, Jens und Kramer, Rudi: EU-DSGVO – Diskussionspunkte aus der Praxis. In: *Datenschutz und Datensicherheit*, Band 37(5): S. 287–294, 2013.

Ehmann, Horst: Informationsschutz und Informationsverkehr im Zivilrecht. In: *Archiv für die civilistische Praxis*, Band 188: S. 230–380, 1988.

Ehmann, Horst: Prinzipien des deutschen Datenschutzrechts – unter Berücksichtigung der Datenschutz-Richtlinie der EG vom 24.10.1995 (1. Teil). In: *Recht der Datenverarbeitung*, Band 14(6): S. 235–243, 1998.

Ehmann, Horst: Prinzipien des deutschen Datenschutzrechts – unter Berücksichtigung der Datenschutz-Richtlinie der EG vom 24.10.1995 (2. Teil). In: *Recht der Datenverarbeitung*, Band 15(1): S. 12–23, 1999.

Ehrenreich, Rosa: Privacy and Power. In: *The Georgetown Law Journal*, Band 89: S. 2047–2062, 2001.

Eifert, Martin: Zweckvereinbarkeit statt Zweckbindung als Baustein eines modernisierten Datenschutzes. In: Gropp, Walter, Lipp, Martin und Steiger, Heinhard (Hg.) *Rechtswissenschaft im Wandel*. Mohr Siebeck, Tübingen, 2007, S. 139–152.

Elahi, Golnaz: Security Requirements Engineering: State of the Art and Practice and Challenges. 2008. URL `http://www.cs.toronto.edu/~gelahi/DepthPaper.pdf`.

Electronic Privacy Information Center und Junkbusters: Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. 2000.

Endres, Elisabeth: Datenerfassung und Probleme der Demokratisierung. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975, S. 63–68.

Enzensberger, Hans Magnus: „Der Sonnenstaat des Doktor Herold“. In: *Spiegel*, (25): S. 68–78, 1979a.

Enzensberger, Hans Magnus: Unentwegter Versuch, einem New Yorker Publikum die Geheimnisse der deutschen Demokratie zu erklären. In: *Kursbuch*, Band 56: S. 1–14, 1979b.

Etzioni, Amitai: A Communitarian Perspective on Privacy. In: *Connecticut Law Review*, Band 32: S. 897–905, 1999a.

Etzioni, Amitai: *The Limits of Privacy*. Basic Books, New York, 1999b.

Etzioni, Amitai: *Privacy in a Cyber Age: Policy and Practice*. Palgrave Macmillan, Basingstoke, 2015.

Europäische Kommission: Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). 2012.

Fabian, Benjamin, Gürses, Seda, Heisel, Maritta, Santen, Thomas und Schmidt, Holger: A comparison of security requirements engineering methods. In: *Requirements engineering*, Band 15(1): S. 7–40, 2010.

Federrath, Hannes und Berthold, Oliver: Identitätsmanagement. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 189–204. 2000.

Federrath, Hannes und Pfitzmann, Andreas: Bausteine zur Realisierung mehrseitiger Sicherheit. In: Müller, Günter und Pfitzmann, Andreas (Hg.) *Mehrseitige Sicherheit in der Kommunikationstechnik*. Addison-Wesley-Longman, 1997, S. 83–104.

Federrath, Hannes und Pfitzmann, Andreas: Die Rolle der Datenschutzbeauftragten bei der Aushandlung von mehrseitiger Sicherheit. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz“ – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 166–172. 1998.

Federrath, Hannes und Pfitzmann, Andreas: Neues Datenschutzrecht und die Technik. In: Kubicek, Herbert, Klumpp, Dieter, Fuchs, Gerhard und Roßnagel, Alexander (Hg.) *Internet@future. Technik, Anwendungen und Dienste der Zukunft*. Hüthig Verlag, Heidelberg, 2001, Band 9 von *Jahrbuch Telekommunikation und Gesellschaft*, S. 252–259.

Feige, Edgar L. und Watts, Harold W.: Protection of Privacy though Microaggregation. In: Bisco, Ralph L. (Hg.) *Data bases, computers, and the social sciences*. John Wiley & Sons, New York, 1970, Information Sciences Series, S. 261–272. Based on papers presented at the Fourth Annual Conference of the Council of Social Science Data Archives held at the University of California in Los Angeles in June, 1967.

Feja, Sven, Witt, Sören, Brosche, Andreas, Speck, Andreas und Prietz, Christian: Modellierung und Validierung von Datenschutzanforderungen in Prozessmodellen. In: *Gemeinsame Fachtagung Verwaltungsinformatik FTVI und Fachtagung Rechtsinformatik FTRI*. Gesellschaft für Informatik, 2010, S. 155–166.

Fiedler, Herbert: Probleme der elektronischen Datenverarbeitung in der öffentlichen Verwaltung. In: *Deutsche Rentenversicherung*, S. 40–47, 1964.

Fiedler, Herbert: Datenschutz und Gesellschaft. In: Siefkes, D. (Hg.) *GI – 4. Jahrestagung*. GI, Gesellschaft für Informatik, Springer, Berlin, Heidelberg, New York, 1975, Band 26 von *Lecture Notes in Computer Science*, S. 68–84.

Fiedler, Herbert: Datenschutz und Gesellschaft. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 179–195. 1976.

Fiedler, Herbert: Vom Datenschutz- zum Informationsrecht. In: *Datenschutz und Datensicherung*, Band 5(1): S. 10–13, 1981.

Finckh, Ute: Resümee. In: Steinmüller, Wilhelm (Hg.) *Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft*, Fischer Taschenbuch Verlag, Frankfurt am Main, S. 197–205. 1988.

Finn, Rachel L., Wright, David und Friedewald, Michael: Seven Types of Privacy. In: Gutwirth, Serge, Leenes, Ronald, De Hert, Paul und Poullet, Yves (Hg.) *European Data Protection: Coming of Age*. Springer, Dordrecht, 2013, S. 3–32.

Fischer-Hübner, Simone: Ein formales Datenschutz-Modell. In: Bauknecht, Kurt (Hg.) *Sicherheit in Informationssystemen*. 1994, S. 107–119.

Fischer-Hübner, Simone: *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*, Band 1958 von *Lecture Notes in Computer Science*. Springer, Berlin, 2001.

Fischer-Hübner, Simone und Ott, Amon: From a Formal Privacy Model to its Implementation. In: *Proceedings of the 21st National Information Systems Security Conference, Arlington, VA*. 1998.

Flaherty, David H.: *Privacy in Colonial New England*. University of Virginia Press, Charlottesville, 1972.

Flaherty, David H.: Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies. In: *Science, Technology, & Human Values*, Band 11(1): S. 7–18, 1986.

Flaherty, David H.: The Emergence of Surveillance Societies in the Western World: Toward the Year 2000. In: *Government Information Quarterly*, Band 5(4): S. 377–387, 1988.

Flaherty, David H.: *Protecting Privacy in Surveillance Societies*. The University of North Carolina Press, Chapel Hill, 1989a.

Flaherty, David H.: Towards the Year 2000: The Emergence of Surveillance Societies in the Western World. In: *Datenschutz und Datensicherung*, Band 13(7): S. 342–347, 1989b.

Flaherty, David H.: Privacy impact assessments: an essential tool for data protection. In: *Privacy Law and Policy Reporter*, 2000. URL `http://www.austlii.edu.au/au/journals/PLPR/2000/45.html`.

Floyd, Christiane: Wo sind Grenzen des verantwortbaren Computereinsatzes? In: Bickenbach, Joachim, Keil-Slawik, Reinhard, Löwe, Michael und Wilhelm, Rudolf (Hg.) *Militarisierte Informatik*, Bund demokratischer Wissenschaftler, Marburg, Nummer 4 in Schriftenreihe Wissenschaft und Frieden, S. 175–180. 1985.

Foddy, W. H.: A critical evaluation of Altman's definition of privacy as a dialectical process. In: *Journal for the Theory of Social Behaviour*, Band 14(3): S. 297–307, 1984.

Foddy, W. H. und Finighan, W. R.: The concept of privacy from a symbolic interaction perspective. In: *Journal for the Theory of Social Behaviour*, Band 10(1): S. 1–17, 1980.

Foschepoth, Josef: *Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik*. Bundeszentrale für politische Bildung, Bonn, 2013.

Foucault, Michel: *Archäologie des Wissens*. Suhrkamp, Frankfurt am Main, 1973.

Fox, Dirk: Datenschutzbeauftragte als „Trusted Third Parties"? In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 81–91. 1998.

Fox, Dirk: Nach der Novelle ist vor der Sanierung. In: *Datenschutz und Datensicherheit*, Band 33(10): S. 583–583, 2009.

Freeman, R. Edward: The Stakeholder Approach Revisited. In: *Zeitschrift für Wirtschafts- und Unternehmensethik*, Band 5(3): S. 228–241, 2004.

Freiherr von Uckermann, Eckart: Einwilligung nach BDSG – ein Mißverständnis? In: *Datenschutz und Datensicherung*, Band 3(3): S. 163–168, 1979.

Freund, Paul A.: Privacy: One Concept or Many. In: Pennock, J. Roland und Chapman, John W. (Hg.) *Privacy*, Atherton Press, New York, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy*, S. 182–198. 1971.

Fried, Charles: Privacy. In: *Yale Law Journal*, Band 77: S. 475–493, 1968.

Friedewald, Michael, Obersteller, Hannah, Nebel, Maxi, Bieker, Felix und Rost, Martin: Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz. White Paper, Forum Privatheit, 2016.

Friedewald, Michael und Wright, David: Safeguards in a World of Ambient Intelligence. Report on the Final Conference, Brussels, 21–22 March 2006. Deliverable D5, SWAMI, 2006.

Friedman, Batya: Value-Sensitive Design. In: *interactions*, Band 3(6): S. 17–23, 1996.

Friedman, Batya (Hg.): *Human Values and the Design of Computer Technology*. Cambridge University Press, Cambridge, 1997.

Friedman, Batya, Felten, Edward und Millett, Lynette I.: Informed Consent Online: A Conceptual Model and Design Principles. Technical Report 00–12–02, University of Washington, Department of Computer Science & Engineering, 2000.

Friedman, Batya, Kahn, Peter H. und Borning, Alan: Value Sensitive Design: Theory and Methods. Technical Report 02–12–01, University of Washington, Department of Computer Science & Engineering, 2002.

Friedrich, Carl J.: Secrecy versus Privacy: The Democratic Dilemma. In: Pennock, J. Roland und Chapman, John W. (Hg.) *Privacy*, Atherton Press, New York, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy*, S. 105–120. 1971.

Frohman, Larry: „Only Sheep Let Themselves Be Counted". Privacy, Political Culture, and the 1983/87 West German Census Boycotts. In: *Archiv für Sozialgeschichte*, Band 52: S. 335–378, 2012.

Froomkin, A. Michael: Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. In: *University of Illinois Law Review*, Band 2015(5): S. 1713–1790, 2015.

Fuster, Gloria González: *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer, Heidelberg, 2014.

Gallagher, Cornelius E.: The computer and the invasion of privacy. In: *Proceedings of the fifth SIGCPR conference on Computer personnel research*. ACM, New York, NY, USA, 1967, SIGCPR '67, S. 108–114. doi:10.1145/1142662.1142676.

Gallie, Walter Bryce: Essentially Contested Concepts. In: *Proceedings of the Aristotelian Society*, Band 56: S. 167–198, 1956.

Gallwas, Hans-Ullrich: Verfassungsrechtliche Grundlagen des Datenschutzes. In: *Der Staat*, Band 18: S. 507–520, 1979.

Gandy, Oscar H., Jr.: The Surveillance Society: Information Technology and Bureaucratic Social Control. In: *Journal of Communication*, Band 39(3): S. 61–76, 1989.

Gandy, Oscar H., Jr.: *The Panoptic Sort*. Westview Press, Boulder, San Francisco, Oxford, 1993.

Garfinkel, Simson: *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly, 2000.

Garrison, William A. und Ramamoorthy, C. V.: Privacy and Security in Data Banks. Technical Memorandum No. 24, Information Systems Research Laboratory, Electronics Research Center, The University of Texas at Austin, Austin, Texas, 1970.

Garstka, Hansjürgen: Grundbegriffe für den Datenschutz. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 209–222. 1973.

Garstka, Hansjürgen: Auswirkungen innovativer Informationsstrukturen auf die Bedeutung und Reichweite verfassungsmäßiger Grundrechte. Arbeitspapier für das Werkstattgespräch „Gesellschaftliche Auswirkungen großer Informationssysteme" der Gesellschaft für Informatik, 29./31.3.77, Hamburg. Arbeitspapier, Freie Universität Berlin, 1977.

Garstka, Hansjürgen: Eine Generation für den Datenschutz, aber wohin? In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 5–14. 2004.

Garstka, Hansjürgen und Coy, Wolfgang (Hg.): *Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis*. Humboldt-Universität zu Berlin, Hermann von Helmholtz-Zentrum für Kulturtechnik, Berlin, 2014.

Gassmann, Hans-Peter: Probleme bei internationalen Datenflüssen und Gemeinsamkeiten des Datenschutzes in Europa. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 11–26. 1976.

Gavison, Ruth: Privacy and the Limits of Law. In: *The Yale Law Journal*, Band 89(3): S. 421–471, 1980.

GegenStandpunkt: Geheim und doch nicht zu übersehen: Die nützlichen Dienste von CIA, BND und Co. für ihre Demokratien. In: *GegenStandpunkt*, Band 2006(1): S. 31–55, 2006.

Geiger, Hansjörg: Datenschutz und Gewaltenteilung. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 173–185. 1973.

Gellert, Raphael und Gutwirth, Serge: The legal construction of privacy and data protection. In: *Computer Law & Security Review*, Band 29: S. 522–530, 2013.

Gellman, Robert: Fair Information Practices: A Basic History. Version 2.10. 2014. URL `http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf`.

Genrich, Hartmann J.: Die Angst vor dem mächtigen Computer: Ist Datenschutz überhaupt erreichbar? In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975, S. 157–161.

Genscher, Hans-Dietrich: Die öffentliche Verwaltung im Kräftefeld der Datenverarbeitung. In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 1(0): S. 4–5, 1971.

George, Joey F. und King, John L.: Examining the computing and centralization debate. In: *Communications of the ACM*, Band 34(7): S. 62–72, 1991.

Gerhardt, Waltraut: Zur Modellierbarkeit von Datenschutzanforderungen im Entwurfsprozeß eines Informationssystems. In: *Datenschutz und Datensicherung*, Band 16(3): S. 126–136, 1992.

Gesellschaft für Informatik: Stellungnahme der Gesellschaft für Informatik (GI) zum Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes. In: *Informatik Spektrum*, S. 112–114, 1984.

Geuss, Raymond: *Public Goods, Private Goods*. Princeton University Press, 2001.

Geuss, Raymond: *Privatheit. Eine Genealogie*. Suhrkamp Verlag, Frankfurt am Main, 2013.

Giesen, Thomas: Kurzes Plädoyer gegen unser Totalverbot: Deine Daten gehören Dir keineswegs! In: *PinG*, (2): S. 62–64, 2013.

Gilliom, John: A response to Bennett's 'In defence of privacy'. In: *Surveillance & Society*, Band 8(4): S. 500–504, 2011.

Giloi, Wolfgang: Der Computer und die Rechte des einzelnen. In: *Datascope*, Band 1(2): S. 1–10, 1970.

Giorgini, Paolo, Massacci, Fabio, Mylopoulos, John und Zannone, Nicola: Requirements Engineering meets Trust Management: Model, Methodology, and Reasoning. Technical Report DIT-04-016, University of Trento, Department of Information and Communication Technology, 2004.

Giorgini, Paolo, Massacci, Fabio, Mylopoulos, John und Zannone, Nicola: Requirements Engineering for Trust Management: Model, Methodology, and Reasoning. In: *International Journal of Information Security*, Band 5(4): S. 257–274, 2006.

Giorgini, Paolo, Massacci, Fabio und Zannone, Nicola: Security and Trust Requirements Engineering. In: *Foundations of Security Analysis and Design III*, S. 237–272, 2005.

Goffman, Erving: *The Presentation of Self in Everyday Life.* University of Edinburgh, Social Sciences Research Centre, Edinburgh, 1956. Monograph No. 2.

Goffman, Erving: *The Presentation of Self in Everyday Life.* Doubleday, New York, 1959.

Gola, Peter (Hg.): *Datenschutz im Konflikt.* Beiheft 13, Datenverarbeitung im Recht (DVR). J. Schweitzer Verlag, München, 1983.

Goldberg, Ian: Privacy-enhancing technologies for the Internet, II: Five years later. In: *Proceedings of the 2nd international conference on Privacy enhancing technologies.* Springer, 2002, S. 1–12.

Goldberg, Ian: Privacy Enhancing Technologies for the Internet III: Ten Years Later. In: Acquisti, Alessandro, Gritzalis, Stefanos, Lambrinoudakis, Costas und De Capitani di Vimercati, Sabrina (Hg.) *Digital Privacy: Theory, Technologies and Practices.* Auerbach Publications, New York, London, 2007, S. 3–18.

Goldberg, Ian, Wagner, David und Brewer, Eric: Privacy-enhancing technologies for the Internet. In: *Proceedings Compcon'97.* IEEE, 1997, S. 103–109.

Golsong, Heribert: Towards a European Convention on Data Protection. In: *Computer Networks*, Band 3: S. 215–218, 1979.

Gotzhein, Reinhard und Horbach, Lothar: Specification and Realization of Protection Problems as Applied to the Erlangen Cancer Registry. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 142–155. 1985.

Gray, Susan H.: Electronic Data Bases and Privacy: Policy for the 1990s. In: *Science, Technology & Human Values*, Band 14(3): S. 242–257, 1989.

Grenier, Edward J., Jr.: Computers and Privacy: A Proposal for Self-Regulation. In: *Duke Law Journal*, Band 1970(3): S. 495–513, 1970.

Grimm, Rüdiger und Roßnagel, Alexander: Can P3P Help to Protect Privacy Worldwide? In: *Proceedings of the 2000 ACM Workshops on Multimedia.* ACM, 2000, S. 157–160.

Grimmelmann, James: Regulation by Software. In: *Yale Law Journal*, Band 114: S. 1719–1758, 2005.

Grimmer, Klaus: Probleme der Institutionalisierung von Informationssystemen im Bereich der öffentlichen Verwaltung. In: Schmitz, P. (Hg.) *Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung.* Gesellschaft für Informatik, Fachausschuß 8 „Methoden der Informatik für spezielle Anwendungen", Springer, Berlin, Heidelberg, New York, 1974, Band 9 von *Lecture Notes in Computer Science*, S. 87–103.

Grimmer, Klaus: Informationsverbund: Öffentlicher und privater Bereich – Problemskizze –. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 66–94. 1976.

Gritzalis, Dimitris A.: Embedding privacy in IT applications development. In: *Information Management & Computer Security*, Band 12(1): S. 8–26, 2004.

Gross, Hyman: Privacy and Autonomy. In: Pennock, J. Roland und Chapman, John W. (Hg.) *Privacy*, Atherton Press, New York, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy*, S. 169–181. 1971.

Gräf, Lorenz: *Privatheit und Datenschutz. Eine soziologische Analyse aktueller Regelungen zum Schutz privater Bereiche auf dem Hintergrund einer Soziologie der Privatheit.* Dissertation, Universität zu Köln, Philosophische Fakultät, Köln, 1993.

Grötker, Ralf: Informationelle Selbstbestimmung – ein zeitgemäßes Leitprinzip? In: Sokol, Bettina (Hg.) *Total transparent – Zukunft der informationellen Mitbestimmung*. LDI NRW, Düsseldorf, 2006, S. 48–64.

Gusy, Christoph: Informationelle Selbstbestimmung und Datenschutz: Fortführung oder Neuanfang? In: *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*, Band 83: S. 52–64, 2000.

Gutwirth, Serge, De Hert, Paul und De Sutter, Laurent: The trouble with technology regulation from a legal perspective: Why Lessig's 'optimal mix' will not work. In: Brownsword, Roger und Yeung, Karin (Hg.) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, Oxford, S. 193–218. 2008.

Gutwirth, Serge und Hildebrandt, Mireille: Some Caveats on Profiling. In: Gutwirth, Serge, Poullet, Yves und De Hert, Paul (Hg.) *Data Protection in a Profiled World*. Springer, Dordrecht, 2010, S. 31–41.

Gärtner, Josef H.: Privatrechtliche Fragen des Datenschutzes. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 70–82. 1976.

Gürses, Seda: PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm. In: *Identity in the Information Society*, Band 3(3): S. 539–563, 2010.

Gürses, Seda und del Alamo, Jose M.: Privacy Engineering: Shaping an Emerging Field of Research and Practice. In: *IEEE Security & Privacy*, Band 14(2): S. 40–46, 2016.

Gürses, Seda, Troncoso, Carmela und Diaz, Claudia: Engineering Privacy by Design. In: *Conference on Computers, Privacy & Data Protection*. 2011. URL `https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf`.

Haefner, Klaus: *Der „Große Bruder". Chancen und Gefahren für eine informierte Gesellschaft*. Econ-Verlag, Düsseldorf, 1980.

Haggerty, Kevin D. und Ericson, Richard V.: The surveillant assemblage. In: *The British journal of sociology*, Band 51(4): S. 605–622, 2000.

Hallinan, Dara, Friedewald, Michael und McCarthy, Paul: Citizens' perceptions of data protection and privacy in Europe. In: *Computer Law & Security Review*, Band 28: S. 263–272, 2012.

Hammer, Volker: *Die 2. Dimension der IT-Sicherheit. Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen*. Vieweg, Braunschweig/Wiesbaden, 1999.

Hammer, Volker: Verletzlichkeitsreduzierende Technikgestaltung. In: *Datenschutz und Datensicherheit*, Band 24(3): S. 137–143, 2000.

Hammer, Volker, Pordesch, Ulrich und Roßnagel, Alexander: KORA. Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für IuK-Systeme. Technischer Bericht 100, provet – Projektgruppe verfassungsverträgliche Technikgestaltung, Darmstadt, 1992.

Hammer, Volker, Pordesch, Ulrich und Roßnagel, Alexander: *Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet*. Springer, Berlin, 1993.

Hansen, Marit: Mit dem Werkzeugkasten in die Informationsgesellschaft. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 283–313. 2004.

Hansen, Marit: Linkage Control — Integrating the Essence of Privacy Protection into Identity Management Systems. In: Cunningham, P. und Cunningham, M. (Hg.) *Collaboration and the Knowledge Economy: Issues, Applications, Case Studies*. IOS Press, Amsterdam, 2008, S. 1585–1592.

Hansen, Marit: Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. In: Camenisch, Jan Leonhard (Hg.) *Privacy and Identity 2011*. 2012, Band 375 von *IFIP AICT*, S. 14–31.

Hansen, Marit: Datenschutz nach dem Summer of Snowden. In: *Datenschutz und Datensicherheit*, Band 38(7): S. 439–444, 2014a.

Hansen, Marit: Hemmnisse für Privacy by Design. In: Pohle, Jörg und Knaut, Andrea (Hg.) *Fundationes I: Geschichte und Theorie des Datenschutzes*. Monsenstein und Vannerdat, Münster, 2014b, S. 73–83.

Hansen, Marit, Berlich, Peter, Camenisch, Jan, Clauß, Sebastian, Pfitzmann, Andreas und Waidner, Michael: Privacy-Enhancing Identity Management. In: *Information Security Technical Report*, Band 9(1): S. 35–44, 2004.

Hansen, Marit, Jensen, Meiko und Rost, Martin: Protection Goals for Privacy Engineering. In: *Proceedings of the International Workshop on Privacy Engineering (IWPE)*. IEEE eXplore, 2015.

Hansen, Marit und Meissner, Sebastian: Verkettung digitaler Identitäten. Technischer Bericht Projektnummer: PLI1563, ULD – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein; Technische Universität Dresden, Professur Datenschutz und Datensicherheit, Kiel, 2007.

Hansen, Marit und Thomsen, Sven: Lebenslanger Datenschutz: Anforderungen an vertrauenswürdige Infrastrukturen. In: *Datenschutz und Datensicherheit*, Band 34(5): S. 283–288, 2010.

Harbird, Rae, Ahmed, Mohamed O., Finkelstein, Anthony, McKinney, Elaine und Burroughs, Andrew: Privacy Impact Assessment with PRAIS. In: *Proceedings of the 8th Privacy Enhancing Technologies Symposium (PETS 2008)*. HotPETS Technical Reports, 2008.

Harbordt, Steffen: Die Gefahr computerunterstützter administrativer Entscheidungsprozesse: Technokratisierung statt Demokratisierung. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975, S. 71–77.

Harrison, Annette: The Problem of Privacy in the Computer Age: An Annotated Bibilography. Memorandum RM-5495-PR/RC, The RAND Corporation, Santa Monica, California, USA, 1967.

Harrison, Annette: The Problem of Privacy in the Computer Age: An Annotated Bibilography. Memorandum RM-5495/1-PR/RC, The RAND Corporation, Santa Monica, California, USA, 1969.

Hartzog, Woodrow: The privacy box: A software proposal. In: *First Monday*, Band 14(11), 2009. URL `http://www.firstmonday.dk/ojs/index.php/fm/article/view/2682`.

Hartzog, Woodrow und Stutzman, Frederic: Obscurity by Design. In: *Washington Law Review*, Band 88: S. 385–418, 2013.

Harvard Law Review: Privacy and Efficient Government: Proposals for a National Data Center. In: *Harvard Law Review*, Band 82(2): S. 400–417, 1968.

Hasselkuss, Andrea und Kaminski, Claus-Jürgen: Persönlichkeitsrecht und Datenschutz. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 109–128. 1973.

Haug, Frigga: *Kritik der Rollentheorie*. Fischer Taschenbuch Verlag, Frankfurt am Main, 1972.

Havighurst, Clark C.: Foreword. In: *Law and Contemporary Problems*, Band 31(2): S. 251–252, 1966.

He, Qingfeng und Antón, Annie I.: A Framework for Modeling Privacy Requirements in Role Engineering. In: *Proceedings of REFSQ: 9th International Workshop on Requirements Engineering – Foundation for Software Quality – Pre-Proceedings*. 2003, S. 115–124.

Heibey, Hanns-Wilhelm, Lutterbeck, Bernd, Rohlfs, Sabine und Töpel, Michael: Einige Bemerkungen zum Zusammenhang von Computereinsatz, Innovation und Gesellschaft. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 298–310. 1976.

Heider, Franz-Peter: Modellierung und Implementation sicherer Bürosysteme. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 70–83. 1985.

Heller, Christian: *Post-Privacy: Prima leben ohne Privatsphäre.* C. H. Beck, München, 2011.

Hellige, Hans Dieter: Von der Hypermedia-Culture zur Cloud-Media-Culture. Der medieninformatische Diskurs im Wandel der digitalen Medienlandschaft. artec-paper Nr. 205, Universität Bremen, artec Forschungszentrum Nachhaltigkeit, 2015.

Hellman, J. J.: Privacy and Information Systems: An Argument and an Implementation. Report P-4298, The RAND Corporation, Santa Clara, California, 1970.

Hensel, Dirk: Die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht: Die Bildung von Persönlichkeitsprofilen und andere Probleme der Vorratsdatenspeicherung. In: *Datenschutz und Datensicherheit*, Band 33(9): S. 527–530, 2009.

Hermann, Thomas, Jahnke, Isa, Kunau, Gabriele und Loser, Kai-Uwe: Der Sociotechnical Walkthrough: Modellierung von Verwaltungsabläufen. In: Schweighofer, Liebwald, Kreuzbauer und Menzel (Hg.) *Informationstechnik in der juristischen Realität: aktuelle Fragen der Rechtsinformatik.* Verlag Österreich, 2004, Band 9 von *Schriftenreihe Rechtsinformatik*, S. 185–188.

Herold, Horst: Polizeiliche Datenverarbeitung und Menschenrechte. In: *Recht und Politik*, (2): S. 79–86, 1980.

Herrmann, Thomas: SeeMe in a nutshell – the semi-structured, socio-technical Modeling Method. 2006.

Herrmann, Thomas, Hoffmann, Marcel, Kunau, Gabriele und Loser, Kai-Uwe: A modelling method for the development of groupware applications as socio-technical systems. In: *Behaviour & Information Technology*, Band 23(2): S. 119–135, 2004.

Hes, Ronald und Borking, John (Hg.): *Privacy-Enhancing Technologies: The Path to Anonymity – Revised Edition.* Registratiekamer, 2000.

Hessen: Datenschutzgesetz. 1970. GVBl. I, 625–627.

Hessische Zentrale für Datenverarbeitung: *Hessen'80 – Großer Hessenplan – Landesentwicklungsplan.* Wiesbaden, 1970.

Hetzer, Wolfgang: Sicherheitsillusion auf Kosten der Freiheit. In: Sokol, Bettina (Hg.) *Total transparent – Zukunft der informationellen Mitbestimmung.* LDI NRW, Düsseldorf, 2006, S. 35–47.

Heußner, Hermann: Datenverarbeitung und Grundrechtsschutz. In: Hohmann, Harald (Hg.) *Freiheitssicherung durch Datenschutz.* Suhrkamp Verlag, Frankfurt am Main, 1987, S. 110–126.

Heylighen, Francis und Joslyn, Cliff: Cybernetics and Second-Order Cybernetics. In: Meyers, R. A. (Hg.) *Encyclopedia of Physical Science & Technology*, Academic Press, New York, Band 4, S. 155–170. Dritte Auflage, 2001.

Hildebrandt, Mireille: Legal and Technological Normativity: more (and less) than twin sisters. In: *Techné*, Band 12(3): S. 169–183, 2008.

Hildebrandt, Mireille und de Vries, Katja (Hg.): *Privacy, Due Process and the Computational Turn*. Routledge, Abingdon, 2013.

Hildebrandt, Mireille und Tielemans, Laura: Data protection by design and technology neutral law. In: *Computer Law & Security Review*, Band 29(5): S. 509–521, 2013.

Hirsch, Burkhard: Gesellschaftliche Folgen staatlicher Überwachung. In: *Datenschutz und Datensicherheit*, Band 32(2): S. 87–91, 2008.

Hirsch, Burkhard: Zu den Anforderungen eines modernen Datenschutzes. In: *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*, Band 94(2): S. 139–152, 2011.

Hirsch, Burkhard, Dichgans, Hans, Kirst, Victor und Genossen: *Entwurf eines Gesetzes zum Schutz vor unbefugter Verwendung personenbezogener Daten (Datenschutzgesetz)*. Deutscher Bundestag, Drs. 6/2885, 1971.

Hirschman, Albert O.: *Exit, Voice, and Loyalty. Responses to Decline in Firms, Organisations, and States*. Harvard University Press, 1970.

Hirshleifer, Jack: Privacy: Its Origin, Function, and Future. In: *The Journal of Legal Studies*, Band 9(4): S. 649–664, 1980.

Hoffman, Lance J. und Miller, William F.: Getting a Personal Dossier from a Statistical Data Bank. In: Hoffman, Lance J. (Hg.) *Security and Privacy in Computer Systems*, Melville Publishing Company, Los Angeles, S. 289–293. 1973. Nachdruck aus: Datamation, 1970.

Hoffmann, Axel, Jandt, Silke, Hoffmann, Holger und Leimeister, Jan Marco: Integration rechtlicher Anforderungen an soziotechnische Systeme in frühe Phasen der Systementwicklung. In: *Proc. MMS*, S. 72–76, 2011.

Hoffmann, Bernhard: *Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes*. Nomos Verlagsgesellschaft, Baden-Baden, 1991.

Hoffmann, Gerd E.: *Computer, Macht und Menschenwürde*. Fischer Taschenbuch Verlag, Frankfurt am Main, aktualisierte ausgabe Auflage, 1979.

Hoffmann, Gerd E., Tietze, Barbara und Steinmüller, Wilhelm (Hg.): *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975.

Hoffmann-Riem, Wolfgang: Informationelle Selbstbestimmung als Grundrecht kommunikativer Entfaltung. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 11–24. 1998.

Holtz, Leif-Erik: Datenschutzkonformes Social Networking: Clique und Scramble! In: *Datenschutz und Datensicherheit*, Band 34(7): S. 439–443, 2010.

Holtz, Leif-Erik und Schallaböck, Jan: Legal Policy Mechanisms. In: Camenisch, Jan Leonhard (Hg.) *Privacy and Identity Management for Life*. Springer, Berlin, 2011, S. 343–354.

Holvast, Jan: History of Privacy. In: Matyás, Vashek, Fischer-Hübner, Simone, Cvrcek, Daniel und Svenda, Petr (Hg.) *The Future of Identity in the Information Society*. IFIP, Springer, Berlin, Heidelberg, 2009, Band 298 von *IFIP Advances in Information and Communication Technology*, S. 13–42.

Hondius, Frits W.: *Emerging data protection in Europe*. North-Holland Publishing Company, Amsterdam, 1975.

Hondius, Frits W. und Sieghart, Paul: Editorial. In: *Computer Networks*, Band 3: S. 147–148, 1979.

Hong, Jason I., Ng, Jennifer D., Lederer, Scott und Landay, James A.: Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. In: *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*. 2004, S. 91–100.

Hoofnagle, Chris Jay: Privacy Self Regulation: A Decade of Disappointment. In: Winn, Jane K. (Hg.) *Consumer Protection in the Age of the Information Economy*, Ashgate, Aldershot, Kapitel 14, S. 379–401. 2006.

Hoofnagle, Chris Jay: Denialists' Deck of Cards: An Illustrated Taxonomy of Rhetoric Used to Frustrate Consumer Protection Efforts. In: *SSRN*, 2007. URL `https://ssrn.com/abstract=962462`.

Hoofnagle, Chris Jay: How the Fair Credit Reporting Act Regulates Big Data. In: *Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet*. 2013.

Hoofnagle, Chris Jay: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS). 2014. URL `http://www.law.berkeley.edu/16452.htm`.

Hornung, Gerrit: Eine Datenschutz-Grundverordnung für Europa? In: *Zeitschrift für Datenschutz*, Band 2(3): S. 99–106, 2012.

Hornung, Gerrit und Hartl, Korbinian: Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit. In: *Zeitschrift für Datenschutz*, Band 4(5): S. 219–225, 2014.

Hubmann, Heinrich: *Das Persönlichkeitsrecht*. Böhlau-Verlag, Münster, Köln, 1953.

Hubmann, Heinrich: *Das Persönlichkeitsrecht*. Böhlau-Verlag, Köln, zweite Auflage, 1967.

Hughes, Eric: A Cypherpunk's Manifesto. 1993. URL `http://www.activism.net/cypherpunk/manifesto.html`.

Hull, Gordon: Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. In: *Ethics and Information Technology*, Band 17(2): S. 89–101, 2015.

humdog: pandora's vox: on community in cyberspace. 1994. Nach The Alphaville Herald, Introducing Humdog: Pandora's Vox Redux, 05.05.2004, URL `http://alphavilleherald.com/2004/05/introducing_hum.html`.

Höckel, Günter und Pfitzmann, Andreas: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 113–127. 1985.

Hölder, Egon (Hg.): *Das Informationsbankensystem – Vorschläge für die Planung und den Aufbau eines allgemeinen arbeitsteiligen Informationsbankensystems für die Bundesrepublik Deutschland*, Band 1. Carl Heymanns Verlag KG, Bonn, 1971. Bericht der interministeriellen Arbeitsgruppe beim Bundesministerium des Innern an die Bundesregierung – „Hölder-Report".

Hümmerich, Klaus: Datenschutz in der Krise. In: Gola, Peter (Hg.) *Datenschutz im Konflikt*, J. Schweitzer Verlag, München, Beiheft 13, Datenverarbeitung im Recht (DVR), S. 55–58. 1983.

Hümmerich, Klaus und Kniffka, Rolf: Die Entwicklung des Datenschutzrechts im Jahre 1978. In: *Neue Juristische Wochenschrift*, (23): S. 1182–1189, 1979.

Iraschko-Luscher, Stephanie: Einwilligung – ein stumpfes Schwert des Datenschutzes? In: *Datenschutz und Datensicherheit*, Band 30(11): S. 706–710, 2006.

Ishii, Kei, Lutterbeck, Bernd und Pallas, Frank: Forking, Scratching und Re-Merging. Forschungsbericht, Technische Universität Berlin, 2008. Version 1.0.2 vom 7. April 2008.

ISTPA: Privacy Framework Version 1.1. Technischer Bericht, International Security, Trust & Privacy Alliance, San Diego, California, 2002.

ISTPA: Analysis of Privacy Principles: Making Privacy Operational. Technischer Bericht, International Security, Trust and Privacy Alliance, 2007. Version 2.0.

Jacobs, Günter: Die Unwirksamkeit der Anonymisierung von Individualdaten – dargestellt am Beispiel der Amtlichen Stundentenstatistik. In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 3: S. 258–261, 1973.

Jarass, Hans D.: Machtverteilung zwischen Parlament und Verwaltung in der Informationsgesellschaft am Beispiel der USA. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975, S. 54–59.

Jaster, Fred: Konzeption zur Datensicherung mittels kryptographischer Codierung. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 126–137. 1976.

Jensen, Carlos, Tullio, Joe, Potts, Colin und Mynatt, Elizabeth D.: STRAP: A Structured Analysis Framework for Privacy. Technical Report GIT-GVU-05-02, Georgia Institute of Technology, 2005.

Johnson, Eric J., Bellman, Steven und Lohse, Gerald L.: Defaults, Framing and Privacy: Why Opting In–Opting Out. In: *Marketing Letters*, Band 13(1): S. 5–15, 2002.

Jorstad, Eric: The Privacy Paradox. In: *William Mitchell Law Review*, Band 27(3): S. 1503–1526, 2001.

Jourard, Sidney M.: Some Psychological Aspects of Privacy. In: *Law and Contemporary Problems*, Band 31(2): S. 307–318, 1966. ISSN 00239186.

Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros: Vorwort. In: Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros (Hg.) *Datenzugang und Datenschutz*, Athenäum, Königstein/Ts., S. IX–XII. 1980.

Kahler, Thomas: Vorratsdatenspeicherung: Wer spricht Recht? In: *Datenschutz und Datensicherheit*, Band 32(7): S. 449–454, 2008.

Kahlert, Anna: Rechtsgestaltung mit der Methode KORA. In: *Datenschutz und Datensicherheit*, Band 38(2): S. 86–92, 2014.

Kaiser, Anna-Bettina: *Die Kommunikation der Verwaltung. Diskurse zu den Kommunikationsbeziehungen zwischen staatlicher Verwaltung und Privaten in der Verwaltungsrechtswissenschaft der Bundesrepublik Deutschland*. Nomos Verlagsgesellschaft, Baden-Baden, 2009.

Kalloniatis, Christos, Kavakli, Evangelia und Gritzalis, Stefanos: Security Requirements Engineering for e-Government Applications: Analysis of Current Frameworks. In: Traunmüller, Roland (Hg.) *EGOV 2004*. Springer, Berlin, Heidelberg, 2004, Band 3183 von *Lecture Notes in Computer Science*, S. 66–71.

Kalloniatis, Christos, Kavakli, Evangelia und Gritzalis, Stefanos: PriS Methodology: Incorporating Privacy Requirements into the System Design Process. In: *5th IEEE International Symposium on Signal Processing and Information Technology*. 2005, S. 18–21.

Kalloniatis, Christos, Kavakli, Evangelia und Gritzalis, Stefanos: Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process. In: *The Second International Conference on Availability, Reliability and Security (ARES 2007)*. IEEE, 2007, S. 1009–1017.

Kamlah, Ruprecht B.: *Right of Privacy. Das allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen*, Band 4 von *Erlanger Juristische Abhandlungen*. Carl Heymanns Verlag KG, Köln, 1969.

Kamlah, Ruprecht B.: Datenüberwachung und Bundesverfassungsgericht. In: *Die Öffentliche Verwaltung*, Band 23(11): S. 361–364, 1970.

Kamlah, Ruprecht B.: Datenschutz im Spiegel der anglo-amerikanischen Literatur. Gutachten, Bundesministerium des Innern, 1971a. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 2.

Kamlah, Ruprecht B.: Der Informationsanspruch des Parlaments im Computerzeitalter (1. Teil). In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 1(1): S. 35–40, 1971b.

Kamlah, Ruprecht B.: Der Informationsanspruch des Parlaments im Computerzeitalter (Schluß). In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 1(2): S. 60–63, 1971c.

Kamlah, Ruprecht B.: Hinweise aus der Rechtsprechung des Bundesverfassungsgerichts zur Regelung eines materiellen Informationsrechts. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 196–206. 1976.

Kamlah, Ruprecht B.: Datenschutz: Konfliktlösung ohne Übertreibung. In: Gola, Peter (Hg.) *Datenschutz im Konflikt*, J. Schweitzer Verlag, München, Beiheft 13, Datenverarbeitung im Recht (DVR), S. 59–77. 1983.

Kamp, Meike und Rost, Martin: Kritik an der Einwilligung. In: *Datenschutz und Datensicherheit*, Band 37(2): S. 80–83, 2013.

Kang, Jerry: Information Privacy in Cyberspace Transactions. In: *Stanford Law Review*, Band 50(4): S. 1193–1294, 1998.

Karg, Moritz: Die Renaissance des Verbotsprinzips im Datenschutz. In: *Datenschutz und Datensicherheit*, Band 37(2): S. 75–79, 2013.

Karhausen, Mark O.: Datenschutz bei Datenbanken für Umfragen. In: Dammann, Ulrich, Karhausen, Mark O., Müller, Paul J. und Steinmüller, Wilhelm (Hg.) *Datenbanken und Datenschutz*, Herder & Herder, Frankfurt am Main, S. 91–110. 1974.

Karhausen, Mark O.: Informationspolitik und Datenschutz. In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation.* Deutsche Verlags-Anstalt, Stuttgart, 1975, S. 78–90.

Karjoth, Günter, Schunter, Matthias und Waidner, Michael: Privacy-enabled Management of Customer Data. In: *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*, Band 51(1): S. 3–9, 2004.

Karjoth, Günther, Schunter, Matthias und Waidner, Michael: Privacy-enabled Services for Enterprises. Technischer Bericht, IBM Research, Zurich Research Laboratory, Rüschlikon, 2002.

Karst, Kenneth L.: 'The Files': Legal Controls over the Accuracy and Accessibility of Stored Personal Data. In: *Law and Contemporary Problems*, Band 31(2): S. 342–376, 1966.

Kauß, Udo: *Der suspendierte Datenschutz bei Polizei und Geheimdiensten.* Campus Verlag, Frankfurt am Main, New York, 1989.

Kavakli, Evangelia: Modeling organizational goals: Analysis of current methods. In: *2004 ACM Symposium on Applied Computing.* 2004, S. 1339–1343.

Kavakli, Evangelia, Kalloniatis, Christos, Loucopoulos, Pericles und Gritzalis, Stefanos: Incorporating privacy requirements into the system design process. In: *Internet Research*, Band 16(2): S. 140–158, 2006.

Kavakli, Evangelia und Loucopoulos, Pericles: Goal Modelling in Requirements Engineering: Analysis and Critique of Current Methods. In: Krogstie, John, Halpin, Terry und Siau, Keng (Hg.) *Information Modeling Methods and Methodologies*. IGI Global, 2005, S. 102–124.

Kenny, Steve und Borking, John: The Value of Privacy Engineering. In: *Journal of Information, Law and Technology*, Band 1, 2002. URL `http://elj.warwick.ac.uk/jilt/02-1/kenny.html`.

Kerkau, Hans-Joachim: Hat die Datenverarbeitung das Datenschutzrecht überholt? – Überlegungen aus der Sicht der Kontrollpraxis. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 84–95. 1985.

Kessel, Werner: Kooperation der Datenschutzbeauftragten mit Hard- und Softwareentwicklern. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 182–189. 1998.

Kieserling, André: *Selbstbeschreibung und Fremdbeschreibung. Beiträge zu einer Soziologie des soziologischen Wissens*. Suhrkamp Verlag, 2004.

Kilian, Wolfgang: Datenschutz in Wirtschaftsunternehmen. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 289–309. 1973.

Kilian, Wolfgang: Integrierte Personalinformationssysteme und Mitbestimmung. In: Lenk, Klaus (Hg.) *Informationsrechte und Kommunikationspolitik*. S. Toeche-Mittler Verlag, Darmstadt, 1976, Band 4 von *Beiträge zur juristischen Informatik*, S. 165–179.

Kilian, Wolfgang: Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung? Zum Modernisierungsgutachten 2002 für den Bundesminister des Innern. In: Bizer, Johann, Lutterbeck, Bernd und Rieß, Joachim (Hg.) *Umbruch von Regelungssystemen in der Informationsgesellschaft. Freundesgabe für Alfred Büllesbach*, S. 151–160. 2002.

Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.): *Datenschutz*, Band 1 von *Beiträge zur juristischen Informatik*. Athenäum-Verlag, Frankfurt am Main, 1973. Juristische Grundsatzfragen beim Einsatz elektronischer Datenverarbeitungsanlagen in Wirtschaft und Verwaltung.

Kirby, M. D.: Data Protection and Law Reform. In: *Computer Networks*, Band 3: S. 149–163, 1979.

Kirby, Michael: Privacy protection, a new beginning: OECD principles 20 years on. In: *Privacy Law and Policy Reporter*, 1999.

Kirby, Michael: Twenty-five Years of Evolving Information Privacy Law—Where Have We Come From and Where Are We Going? In: *Prometheus*, Band 21(4): S. 467–475, 2003.

Kirby, Michael: The history, achievement and future of the 1980 OECD guidelines on privacy. In: *International Data Privacy Law*, Band 1(1): S. 6–14, 2011.

Kirtley, Jane E. (Hg.): *The Privacy Paradox*. 1998.

Kiyavitskaya, Nadzeya, Krausová, Alzbeta und Zannone, Nicola: Why Eliciting and Managing Legal Requirements Is Hard. In: *Requirements Engineering and Law (RELAW'08)*. IEEE, 2008, S. 26–30.

Kizza, Joseph Migga: *Ethical and Social Issues in the Information Age*. Springer, New York, 1998.

Klaus, Georg (Hg.): *Wörterbuch der Kybernetik*. Fischer Bücherei, Frankfurt am Main, 1969. 2 Bände.

Kling, Rob und Iacono, Suzanne: The institutional character of computerized information systems. In: *Office: Technology and People*, Band 5(1): S. 7–28, 1989.

Klitou, Demetrius: A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design. In: Preneel, Bart und Ikonomou, Demosthenes (Hg.) *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers*. Springer, Berlin, 2014, S. 86–110.

Kloepfer, Michael: *Datenschutz als Grundrecht*. Athenäum, Königsstein/Ts., 1980.

Kloepfer, Michael: *Geben moderne Technologien und die europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen?: Gutachten D für den 62. Deutschen Juristentag*. C. H. Beck, München, 1998.

Klug, Christoph: Die Vorabkontrolle – Eine neue Aufgabe für betriebliche und behördliche Datenschutzbeauftragte. In: *Recht der Datenverarbeitung*, (1): S. 12–20, 2001.

Kohler, Josef: *Das Autorrecht*. Verlag Gustav Fischer, Jena, 1880.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Eckpunkte zur Reform des Datenschutzrechts. In: *Datenschutz und Datensicherheit*, Band 34(5): S. 331, 2010.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Das Standard-Datenschutzmodell: Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. 2015. URL `https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Handbuch_V09a.pdf`.

Konvitz, Milton R.: Privacy and the Law: A Philosophical Prelude. In: *Law and Contemporary Problems*, Band 31(2): S. 272–280, 1966.

Koops, Bert-Jaap: The (In)Flexibility of Techno-Regulation and the Case of Purpose-Binding. In: *Legisprudence*, Band 5(2): S. 171–194, 2011.

Koops, Bert-Jaap: On decision transparency, or how to enhance data protection after the computational turn. In: Hildebrandt, Mireille und de Vries, Katja (Hg.) *Privacy, Due Process and the Computational Turn*. Routledge, Abingdon, 2013, S. 196–220.

Koops, Bert-Jaap: The trouble with European data protection law. In: *International Data Privacy Law*, Band 4(4): S. 250–261, 2014.

Koops, Bert-Jaap und Leenes, Ronald: Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection Law. In: *International Review of Law, Computers & Technology*, Band 27, 2013. URL `http://www.tandfonline.com/doi/abs/10.1080/13600869.2013.801589`.

Koops, Bert-Jaap, Newell, Bryce Clayton, Timan, Tjerk, Škorvánek, Ivan, Chokrevski, Tom und Galič, Maša: A Typology of Privacy. In: *SSRN*, 2016. URL `https://ssrn.com/abstract=2754043`.

Korba, Larry und Kenny, Steve: Towards Meeting the Privacy Challenge: Adapting DRM. Paper NRC 44956, National Research Council of Canada, Ottawa, 2002.

Korenhof, Paulan, Ausloos, Jef, Szekely, Ivan, Ambrose, Meg, Sartor, Giovanni und Leenes, Ronald: Timing the Right to Be Forgotten: A Study into „Time“ as a Factor in Deciding About Retention or Erasure of Data. In: Gutwirth, Serge, Leenes, Ronald und De Hert, Paul (Hg.) *Reforming European Data Protection Law*. Springer, Dordrecht, 2015.

Koslowski, Knut: *Unterstützung von partizipativer Systementwicklung durch Methoden des Software Engineering*. Nummer 3 in Sozialvertragliche Technikgestaltung. Westdeutscher Verlag, Opladen, 1988.

Kramer, Philipp: Verbot mit Erlaubnisvorbehalt zeitgemäß? In: *Datenschutz und Datensicherheit*, Band 37(6): S. 380–382, 2013.

Krauch, Helmut: Einleitung: Staat und Individuum in der Informationsgesellschaft. In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation.* Deutsche Verlags-Anstalt, Stuttgart, 1975a, S. 7–9.

Krauch, Helmut (Hg.): *Erfassungsschutz.* Deutsche Verlags-Anstalt, Stuttgart, 1975b.

Krause, Harry D.: The Right to Privacy in Germany: Pointers for American Legislation? In: *Duke Law Journal*, Band 1965(3): S. 481–530, 1965.

Krückeberg, Fritz: Unterstützung von Datenschutz und Datensicherung durch Prüfung von Software auf Normkonformität. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 188–204. 1985.

Kubicek, Herbert: Der Mythos der Informationsgesellschaft. Von der Illusion, durch Techniken der Telekommunikation Beschäftigung und neue Freiheiten zu sichern. In: *Gewerkschaftliche Monatshefte*, (6): S. 344–360, 1986.

Kubicek, Herbert: Telematische Integration: Zurück in die Sozialstrukturen des Früh-Kapitalismus? In: Steinmüller, Wilhelm (Hg.) *Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft*, Fischer Taschenbuch Verlag, Frankfurt am Main, S. 51–104. 1988.

Kubicek, Herbert und Rolf, Arno: *Mikropolis. Mit Computernetzen in die „Informationsgesellschaft“.* VSA-Verlag, Hamburg, 1985.

Kuhn, Thomas S.: *The Structure of Scientific Revolutions.* The University of Chicago Press, Chicago, London, dritte Auflage, 1996.

Kulk, Stefan und Borgesius, Frederik Zuiderveen: Google Spain v. Gonzalez: Did the Court Forget about Freedom of Expression. In: *European Journal of Risk Regulation*, Band 5(3): S. 389–398, 2014.

Kuner, Christopher: Reality and Illusion in EU Data Transfer Regulation Post Schrems. Research Paper 14/2016, University of Cambridge, Faculty of Law, Cambridge, 2016.

Kuner, Christopher, Cate, Fred H., Millard, Christopher und Svantesson, Dan Jerker B.: The challenge of 'big data' for data protection. In: *International Data Privacy Law*, Band 2(2): S. 47–49, 2012.

Kung, Antonio: ICT and Privacy: Barriers. In: Preneel, Bart und Ikonomou, Demosthenes (Hg.) *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers.* Springer, Berlin, 2014, S. 177–186.

Kutscha, Martin: Datenschutz durch Zweckbindung – ein Auslaufmodell? In: *Zeitschrift für Rechtspolitik*, (4): S. 156–160, 1999.

Köhntopp, Kristian, Köhntopp, Marit und Pfitzmann, Andreas: Sicherheit durch Open Source? Chancen und Grenzen. In: *Datenschutz und Datensicherheit*, Band 24(9): S. 508–513, 2000.

Kühl, Stefan: *Organisationen: Eine sehr kurze Einführung.* VS Verlag für Sozialwissenschaften, Wiesbaden, 2011.

Ladeur, Karl Heinz: Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken. In: *Datenschutz und Datensicherheit*, Band 24(1): S. 12–19, 2000.

Langheinrich, Marc: Privacy in Ubiquitous Computing. 2009. URL `www.ee.oulu.fi/~vassilis/courses/ubicomp10S/papers/privacy_security/langheinrich-09.pdf`.

Lapouchnian, Alexei: Goal-Oriented Requirements Engineering: An Overview of the Current Research. Research paper, Department of Computer Science, University of Toronto, Toronto, Canada, 2005. URL `http://www.cs.utoronto.ca/~alexei/pub/Lapouchnian-Depth.pdf`.

LaRose, Robert und Rifon, Nora: Your privacy is assured – of being disturbed: websites with and without privacy seals. In: *new media & society*, Band 8(6): S. 1009–1029, 2006.

Laudon, Kenneth C.: Privacy and Federal Data Banks. In: *Society*, Band 17(2): S. 50–56, 1980.

Laudon, Kenneth C.: Data quality and due process in large interorganizational record systems. In: *Communications of the ACM*, Band 29(1): S. 4–11, 1986a.

Laudon, Kenneth C.: *Dossier Society: Value Choices in the Design of National Information Systems*. Columbia University Press, New York, 1986b.

Laudon, Kenneth C.: Markets and Privacy. In: *Communications of the ACM*, Band 39(9): S. 92–104, 1996.

Lederer, Scott, Hong, Jason I., Dey, Anind K. und Landay, James A.: Personal privacy through understanding and action: five pitfalls for designers. In: *Personal and Ubiquitous Computing*, Band 8(6): S. 440–454, 2004.

Lee, L.T.: On-line Anonymity: A New Privacy Battle In Cyberspace. In: *The New Jersey Journal of Communication*, Band 4(2): S. 127–146, 1996.

Leib, Hans-Jürgen: Technische Entwicklung und Datenschutzrecht. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 218–228. 1985.

Lemke, Günter: Sechzehn Thesen zum Thema »Informationsballung in Datenbanken und die qualitative Veränderung von Information«. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975, S. 162–165.

Lenk, Klaus: Legal and Organisational Aspects of Data Protection in Public Administration. In: *Data Banks and Society*, Universitetsforlaget, Oslo, S. 3–17. 1972.

Lenk, Klaus: Datenschutz in der öffentlichen Verwaltung. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 15–50. 1973.

Lenk, Klaus: Wie lassen sich (de-)zentralisatorische Wirkungen der Verwaltungsautomation bestimmen? In: Schmitz, P. (Hg.) *Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung*. Gesellschaft für Informatik, Fachausschuß 8 „Methoden der Informatik für spezielle Anwendungen“, Springer, Berlin, Heidelberg, New York, 1974, Band 9 von *Lecture Notes in Computer Science*, S. 124–133.

Lenk, Klaus: Probleme des Informationsschutzes bei der Breitbandkommunikation. In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation*. Deutsche Verlags-Anstalt, Stuttgart, 1975, S. 91–104.

Lenk, Klaus (Hg.): *Informationsrechte und Kommunikationspolitik*, Band 4 von *Beiträge zur juristischen Informatik*. S. Toeche-Mittler Verlag, Darmstadt, 1976.

Lenk, Klaus: Information Technology and Society. In: Friedrichs, Günter und Schaff, Adam (Hg.) *Microelectronics and Society. For Better or for Worse. A Report to the Club of Rome*. The Club of Rome, Pergamon Press, Oxford, 1982, S. 273–310.

Lenk, Klaus: Perspektiven der ununterbrochenen Informatisierung der Verwaltung. In: *dms – der moderne staat – Zeitschrift für Public Policy, Recht und Management*, Band 4(2): S. 315–334, 2011.

Lenk, Klaus: Gedanken zur Gestaltung technikdurchtränkter Arbeitsorganisation. In: Fuchs-Kittowski, Frank und Kriesel, Werner (Hg.) *Informatik und Gesellschaft. Festschrift zum 80. Geburtstag von Klaus Fuchs-Kittowski.* Peter Lang, 2016, S. 351–360.

Lenk, Klaus, Brüggemeier, Martin, Hehmann, Margret und Willms, Werner: *Bürgerinformationssysteme – Strategien zur Steigerung der Verwaltungstransparenz und der Partizipationschancen der Bürger.* Nummer 10 in Sozialverträgliche Technikgestaltung. Westdeutscher Verlag, Opladen, 1990.

Lessig, Lawrence: *Code and other laws of cyberspace.* Basic Books, New York, 1999.

Li, Ninghui, Li, Tiancheng und Venkatasubramanian, Suresh: t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In: *23rd International Conference on Data Engineering (ICDE 2007).* IEEE, 2007, S. 106–115.

Liedtke, Werner: *Das Bundesdatenschutzgesetz. Eine Fallstudie zum Gesetzgebungsprozeß.* Dissertation, Ludwig-Maximilians-Universität zu München, München, 1980.

Linn, John und Kent, Stephen T.: Electronic mail privacy enhancement. In: *Advances in Computer System Security*, Band 3: S. 327–330, 1988.

Lioudakis, Georgios V., Koutsoloukas, Eleftherios A., Dellas, Nikolaos L., Tselikas, NNikolaos, Kapellaki, Sofia, Prezerakos, George N., Kaklamani, Dimitra I. und Venieris, Iakovos S.: A middleware architecture for privacy protection. In: *Computer Networks*, Band 51(16): S. 4679–4696, 2007.

Liu, Lin, Yu, Eric und Mylopoulos, John: Security and Privacy Requirements Analysis within a Social Setting. In: *11th IEEE International Requirements Engineering Conference, 2003. Proceedings.* 2003, S. 151–161.

Lohmar, Ulrich: Datenschutz als Tarnkappe der Staatsbürokratie? In: Gola, Peter (Hg.) *Datenschutz im Konflikt*, J. Schweitzer Verlag, München, Beiheft 13, Datenverarbeitung im Recht (DVR), S. 91–104. 1983.

Losbichler, Bruno: Zugriff zu schutzbedürftigen Objekten in Programmen. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 138–154. 1976.

Luhmann, Niklas: *Funktionen und Folgen formaler Organisation.* Duncker & Humblot, Berlin, 1964a.

Luhmann, Niklas: Zweck – Herrschaft – System. Grundbegriffe und Prämissen Max Webers. In: *Der Staat*, Band 3(2): S. 129–158, 1964b.

Luhmann, Niklas: *Recht und Automation in der öffentlichen Verwaltung*, Band 29 von *Schriftenreihe der Hochschule Speyer.* Duncker & Humblot, Berlin, 1966a.

Luhmann, Niklas: *Theorie der Verwaltungswissenschaft: Bestandsaufnahme und Entwurf.* G. Grote'sche Verlagsbuchhandlung KG, Köln, Berlin, 1966b.

Luhmann, Niklas: *Legitimation durch Verfahren.* Hermann Luchterhand Verlag, Neuwied, Berlin, 1969.

Luhmann, Niklas: Verfassungsmäßige Auswirkungen der elektronischen Datenverarbeitung. In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 2(2): S. 44–47, 1972.

Luhmann, Niklas: *Zweckbegriff und Systemrationalität.* Suhrkamp Verlag, zweite Auflage, 1977.

Luhmann, Niklas: *Soziologische Aufklärung: Soziales System, GeselIschaft, Organisation*, Band 3. Westdeutscher Verlag, Opladen, zweite Auflage, 1981.

Luhmann, Niklas: *Grundrechte als Institution.* Nummer 24 in Schriften zum Öffentlichen Recht. Duncker & Humblot, Berlin, dritte Auflage, 1986. Unveränderter Nachdruck der 1965 erschienenen ersten Auflage.

Luhmann, Niklas: *Soziale Systeme. Grundriß einer allgemeinen Theorie.* Suhrkamp Taschenbuch Verlag, Frankfurt am Main, 1987.

Luhmann, Niklas: *Die Realität der Massenmedien*, VS Verlag für Sozialwissenschaften, Wiesbaden, S. 5–73. 1995.

Luhmann, Niklas: *Organisation und Entscheidung.* Westdeutscher Verlag, Opladen/Wiesbaden, 2000.

Lutterbeck, Bernd: Entscheidungstheoretische Bemerkungen zum Gewaltenteilungsprinzip. Zur Problematik parlamentarischer Informationsrechte im Datenschutz. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 187–206. 1973.

Lutterbeck, Bernd: Informationelle Probleme parlamentarischer Beteiligung an Planungsprozessen. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 164–178. 1976.

Lutterbeck, Bernd: 20 Jahre Dauerkonflikt: Die Novellierung des Bundesdatenschutzgesetzes. In: Sokol, Bettina (Hg.) *20 Jahre Datenschutz – Individualismus oder Gemeinschaftssinn.* Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Düsseldorf, 1998a, S. 7–34.

Lutterbeck, Bernd: 20 Jahre Dauerkonflikt: Die Novellierung des Bundesdatenschutzgesetzes. In: *Datenschutz und Datensicherheit*, Band 22(3): S. 129–138, 1998b.

Lutterbeck, Bernd: Internet Governance. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 47–57. 2000.

Lutterbeck, Bernd: Das informationelle Selbstbestimmungsrecht auf dem Prüfstand: 7 Schritte auf dem Weg zu einem zukunftsfähigen Datenschutz. Notizen für das 5. Datenschutzkolloquium der SCHUFA. 2010. URL `http://lutterbeck.org/data/uploads/lutterbeck_isr-28092010-1.1.pdf`.

Lutz, Christoph und Strathoff, Pepe: Privacy Concerns and Online Behavior – Not so Paradox After All? Viewing the Privacy Paradox through different theoretical lenses. In: Brändli, Sandra, Schister, Roman und Tamò, Aurelia (Hg.) *Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft.* Universität Sankt Gallen, Stämpfli, Bern, 2013, Band 8 von *Schriften der Assistierenden der Universität St. Gallen (HSG)*, S. 81–99.

Lyon, David: *The Electronic Eye: The Rise of Surveillance Society.* University of Minnesota Press, Minneapolis, 1994.

Lyon, David: Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix. In: *Surveillance & Society*, Band 1(1): S. 1–7, 2002.

Lyon, David und Zureik, Elia (Hg.): *Computers, Surveillance, and Privacy.* University of Minnesota Press, Minneapolis, 1996.

Löchner, Gerhard: Datenschutz und Datensicherung, erläutert am Bundeszentralregister. In: Löchner, Gerhard und Steinmüller, Wilhelm (Hg.) *Datenschutz und Datensicherung.* Deutsche Sektion der Internationalen Juristen-Kommission, C. F. Müller Verlag, Karlsruhe, 1975, Band 1 von *Rechtsstaat in der Bewährung*, S. 1–33.

Löchner, Gerhard und Steinmüller, Wilhelm (Hg.): *Datenschutz und Datensicherung*, Band 1 von *Rechtsstaat in der Bewährung*. Deutsche Sektion der Internationalen Juristen-Sektion, C. F. Müller Verlag, Karlsruhe, 1975.

Maass, Hans-Heinrich: *Information und Geheimnis im Zivilrecht*, Band 4 von *Münchener Universitätsschriften – Abhandlungen des Instituts für europäisches und internationales Wirtschaftsrecht*. Ferdinand Enke Verlag, Stuttgart, 1970.

Machanavajjhala, A., Kifer, D., Gehrke, J. und Venkitasubramaniam, M.: l-Diversity: Privacy Beyond k-Anonymity. In: *ACM Transactions on Knowledge Discovery from Data (TKDD)*, Band 1(1), 2007. Artikel Nr. 3.

Mallmann, Christoph: Das Problem der Privatsphäre innerhalb des Datenschutzes. In: Schneider, Jochen (Hg.) *Datenschutz – Datensicherung*, Siemens Aktiengesellschaft, München, Heft 5 Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung, Kapitel 3, S. 19–26. 1971.

Mallmann, Christoph: *Datenschutz in Verwaltungs-Informationssystemen*, Band 2 von *Rechtstheorie und Informationsrecht*. R. Oldenbourg Verlag, München, Wien, 1976a.

Mallmann, Otto: Soziale Kontrolle durch Breitbandtechnologien. In: Lenk, Klaus (Hg.) *Informationsrechte und Kommunikationspolitik*. S. Toeche-Mittler Verlag, Darmstadt, 1976b, Band 4 von *Beiträge zur juristischen Informatik*, S. 125–136.

Mallmann, Otto: *Zielfunktionen des Datenschutzes*. Dissertation, Johann-Wolfgang-Goethe-Universität, Fachbereich Rechtswissenschaft, Frankfurt am Main, 1977.

Manske, Phillipp: Unbekannte Umweltaktivistin muss für zwei Monate in Haft. In: *RBB Online*, 2016. 09.06.2016, URL `https://www.rbb-online.de/wirtschaft/thema/braunkohle/beitraege/unbekannte-umweltaktivistin-vor-gericht-braunkohleproteste-lausi.html`.

Mansmann, Urs: Gestrandet ohne Internet: O2 verpatzt den Umzug eines DSL-Anschlusses. In: *c't – magazin für computer technik*, (14): S. 74–75, 2016.

Mantelero, Alessandro: Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. In: *Computer Law & Security Review*, Band 32(2): S. 238–255, 2016.

Marcuse, Herbert: *Der eindimensionale Mensch: Studien zur Ideologie der fortgeschrittenen Industriegesellschaft*. Hermann Luchterhand Verlag, Neuwied, 1970.

Margulis, Stephen T.: On the Status and Contribution of Westin's and Altman's Theories of Privacy. In: *Journal of Social Issues*, Band 59(2): S. 411–429, 2003.

Margulis, Stephen T.: Three Theories of Privacy: An Overview. In: Trepte, S. und Reinecke, L. (Hg.) *Privacy Online*, Springer, Berlin, Heidelberg, Kapitel 2, S. 9–17. 2011.

Martin, James und Norman, Adrian R. D.: *Halbgott Computer*. BLV Verlagsgesellschaft, München, 1972. The Computerized Society, Prentice Hall, Englewood Cliffs, 1970.

Marwedel, H.: Die Rolle der elektronischen Datenverarbeitung in Planungs- und Entscheidungsprozessen. In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 3(8): S. 343–352, 1973.

Marx, Gary T.: The Surveillance Society – The Threat of 1984-style Techniques. In: *Futurist*, Band 19(3): S. 21–26, 1985.

Marx, Gary T.: Murky conceptual waters: The public and the private. In: *Ethics and Information Technology*, Band 3: S. 157–169, 2001.

Marx, Gary T.: What's New About the „New Surveillance"? Classifying for Change and Continuity. In: *Surveillance & Society*, Band 1(1): S. 9–29, 2002.

Marx, Gary T.: Surveillance Studies. In: Wright, James D. (Hg.) *International Encyclopedia of the Social & Behavioral Sciences*, Elsevier, Amsterdam, S. 733–741. Zweite Auflage, 2015.

Marx, Gary T. und Reichman, Nancy: Routinizing the Discovery of Secrets: Computers as Informants. In: *The American Behavioral Scientist*, Band 27(4): S. 423, 1984.

Marx, Karl und Engels, Friedrich: *Werke*. Dietz Verlag, Berlin, 1974.

Masing, Johannes: Herausforderungen des Datenschutzes. In: *Neue Juristische Wochenschrift*, Band 65(32): S. 2305–2311, 2012.

Massacci, Fabio, Prest, Marco und Zannone, Nicola: Using a Security Requirements Engineering Methodology in Practice: The compliance with the Italian Data Protection Legislation. Technical Report DIT-04-103, Department of Information and Communication Technology, University of Trento, Trento, Italien, 2004.

Massey, Aaron K., Otto, Paul N., Hayward, Lauren J. und Antón, Annie I.: Evaluating existing security and privacy requirements for legal compliance. In: *Requirements engineering*, Band 15(1): S. 119–137, 2010.

Massing, Otwin: Von der Volkszählungsbewegung zur Verrechtlichung oder: Öffentlichkeit, Herrschaftsrationalisierung und Verfahren. In: Hohmann, Harald (Hg.) *Freiheitssicherung durch Datenschutz*. Suhrkamp Verlag, Frankfurt am Main, 1987, S. 85–109.

Masuda, Yoneji: Privacy in the Future Information Society. In: *Computer Networks*, Band 3: S. 164–170, 1979.

Matley, Ben G.: Computer Privacy in America: Conflicting Practices and Policy Choices. In: *IEEE Symposium on Security and Privacy*, S. 219–223, 1985.

Mayer-Schönberger, Viktor: Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing. Research Working Paper RWP07-022, Harvard University, John F. Kennedy School of Government, Cambridge, MA, 2007.

Mayer-Schönberger, Viktor: *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, Princeton, 2009.

Mayer-Schönberger, Viktor und Cukier, Kenneth: *Big Data : A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt, Boston, 2013.

McLuhan, Marshall: *The Gutenberg Galaxy: The Making of Typographic Man*. University of Toronto Press, Toronto, 1962.

Mead, George Herbert: *Mind, Self and Society*. University of Chicago Press, Chicago, 1934.

Meints, Martin: Datenschutz nach BSI-Grundschutz? In: *Datenschutz und Datensicherheit*, Band 30(1): S. 13–16, 2006.

Meints, Martin: Datenschutz durch Prozesse. In: *Datenschutz und Datensicherheit*, Band 31(2): S. 91–95, 2007.

Meister, Herbert: Das Schutzgut des Datenrechts. In: *Datenschutz und Datensicherung*, Band 7(3): S. 163–180, 1983.

Meldman, Jeffrey A.: Centralized Information Systems and the Legal Right to Privacy. In: *Marquette Law Review*, Band 52(3): S. 335–354, 1969.

Mertens, Peter: Das Ungleichgewicht im Datenschutz. In: *Informatik Spektrum*, Band 29(6): S. 416–423, 2006.

Merton, Robert K.: *Social Theory and Social Structure*. The Free Press, New York, 1949.

Miller, Arthur Raphael: The National Data Center and Personal Privacy. In: *The Atlantic*, Band 220(5): S. 53–57, 1967.

Miller, Arthur Raphael: Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society. In: *Michigan Law Review*, Band 67(6): S. 1089–1246, 1969.

Miller, Arthur Raphael: *The Assault on Privacy*. The University of Michigan Press, Ann Arbour, 1971.

Mills, C. Wright: *White Collar: The American Middle Classes*. Oxford University Press, New York, 1951. Nachdruck von 1953.

Minsky, Naftaly H. und Rozenshtein, David: System = Program + Users + Law. In: *Proceedings of the 1st International Conference on Artificial Intelligence and Law*. New York, NY, 1987, ICAIL '87, S. 170–180.

Mont, Marco Casassa, Pearson, Siani und Bramhall, Pete: Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. In: *Proceedings of the 14th International Workshop on Database and Expert Systems Applications*. IEEE Computer Society, Washington, DC, USA, 2003a, DEXA '03, S. 377–382.

Mont, Marco Casassa, Pearson, Siani und Bramhall, Pete: Towards Accountable Management of Privacy and Identity Information. In: Snekkenes, Einar und Gollmann, Dieter (Hg.) *Computer Security – ESORICS 2003*. Springer, Berlin, 2003b, Band 2808 von *Lecture Notes in Computer Science*, S. 146–161.

Mont, Marco Casassa, Thyne, Robert, Chan, K. und Bramhall, P.: Extending HP Identity Management Solutions to Enforce Privacy Policies and Obligations for Regulatory Compliance by Enterprises. Technical Report HPL-2005-110, Trusted Systems Laboratory, HP Laboratories Bristol, Bristol, 2005.

Morningstar, Chip: How To Deconstruct Almost Anything. 1993. URL `http://www.fudco.com/chip/deconstr.html`.

Moser-Knierim, Antonie: *Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr*. Springer Vieweg, Wiesbaden, 2014.

Mulligan, Deirdre K., Koopman, Colin und Doty, Nick: Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. In: *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, Band 374(2083), 2016. doi:10.1098/rsta.2016.0118.

Murphy, Maria Helen: The pendulum effect: comparisons between the Snowden revelations and the Church Committee. What are the potential implications for Europe? In: *Information & Communications Technology Law*, Band 23(3): S. 192–219, 2014.

Mückenberger, Ulrich: Datenschutz als Verfassungsgebot. In: *Kritische Justiz*, S. 1–24, 1984.

Mühlbauer, Peter: Kinderschutz als Vorwand für Politikerschutz? In: *telepolis*, 2014. URL `http://www.heise.de/tp/artikel/41/41500/`.

Müller, Paul J.: Administrative Datenbanken und die zu schützende Privatsphäre. In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 3(2): S. 61–65, 1973.

Müller, Paul J.: Die Gefährdung der Privatsphäre durch Datenbanken. In: Dammann, Ulrich, Karhausen, Mark O., Müller, Paul J. und Steinmüller, Wilhelm (Hg.) *Datenbanken und Datenschutz*, Herder & Herder, Frankfurt am Main, S. 63–90. 1974.

Müller, Paul J.: Einige soziale Auswirkungen integrierter Informationssysteme – Zur Notwendigkeit von Informationskontrolle innerhalb einer Informationspolitik. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975a, S. 121–137.

Müller, Paul J.: Funktionen des Datenschutzes aus soziologischer Sicht. In: *Datenverarbeitung im Recht*, Band 4: S. 107–118, 1975b.

Müller, Paul J.: Soziale Kontrolle durch Datenbanken? In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation*. Deutsche Verlags-Anstalt, Stuttgart, 1975c, S. 141–152.

Müller, Paul J.: Informationsflüsse und Informationshaushalte. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 95–109. 1976.

Müller, Paul J.: Datentreuhänder – Ein Plädoyer für eine volle Ausschöpfung von Datenschutz-Maßnahmen. In: Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros (Hg.) *Datenzugang und Datenschutz*, Athenäum, Königstein/Ts., S. 225–234. 1980.

Müller, Paul J. und Kuhlmann, H. H.: Integrated information bank systems, social book-keeping and privacy. In: *International Social Science Journal*, Band 24(3): S. 584–602, 1972.

Narayanan, Arvind und Shmatikov, Vitaly: Myths and fallacies of „Personally Identifiable Information“. In: *Communications of the ACM*, Band 53(6): S. 24–26, 2010.

Narayanan, Arvind, Toubiana, Vincent, Barocas, Solon, Nissenbaum, Helen und Boneh, Dan: A Critical Look at Decentralized Personal Data Architectures. In: *arXiv preprint arXiv:1202.4503*, 2012.

Narr, Wolf-Dieter: Anmerkungen zu einigen Thesen von W. Steinmüller. In: *Leviathan*, Band 4(3): S. 544–549, 1975.

Newell, Bryce Clayton: The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe. In: *I/S: A Journal of Law and Policy for the Information Society*, Band 10, 2014.

Newman, Nathan: Search, Antitrust, and the Economics of the Control of User Data. In: *Yale Journal on Regulation*, Band 31(2): S. 401–454, 2014.

Nguyen, David H. und Mynatt, Elizabeth D.: Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems. GVU Technical Report GIT-GVU-02-16, Georgia Institute of Technology, Atlanta, Georgia, 2002. URL `http://hdl.handle.net/1853/3268`.

Niblett, G. B. F.: *Digital Information and the Privacy Problem*, Band 2 von *OECD Informatics Studies*. O.E.C.D. Publications, Paris, 1971.

Nissenbaum, Helen: Toward an Approach to Privacy in Public: Challenges of Information Technology. In: *Ethics & Behavior*, Band 7(3): S. 207–219, 1997.

Nissenbaum, Helen: Protecting Privacy in an Information Age: The Problem of Privacy in Public. In: *Law and Philosophy*, Band 17(5/6): S. 559–596, 1998.

Nissenbaum, Helen: Privacy as contextual integrity. In: *Washington Law Review*, Band 79: S. 101–139, 2004.

Nissenbaum, Helen: *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, California, 2010.

Nodorf, Matthias: *Datenschutz in der gesetzlichen Krankenversicherung*. Peter Lang, Frankfurt am Main, 1995.

Nora, Simon und Minc, Alain: *Die Informatisierung der Gesellschaft*. Campus Verlag, Frankfurt am Main, 1979.

Norberg, Patricia A., Horne, Daniel R. und Horne, David A.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. In: *Journal of Consumer Affairs*, Band 41(1): S. 100–126, 2007.

Notario, Nicolás, Crespo, Alberto, Martín, Yod-Samuel, Del Alamo, Jose M, Le Métayer, Daniel, Antignac, Thibaud, Kung, Antonio, Kroener, Inga und Wright, David: PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. In: *2015 IEEE Security and Privacy Workshops (SPW)*. 2015, S. 151–158.

Novotny, Alexander und Spiekermann, Sarah: Personal Information Markets AND Privacy: A New Model to Solve the Controversy. In: Alt, Rainer und Franczyk, Bogdan (Hg.) *Tagungsband der 11. Internationalen Tagung Wirtschaftsinformatik (WI 2013)*. Leipzig, 2013, S. 1635–1649.

Ochs, Carsten und Ilyes, Petra: Sociotechnical Privacy. Mapping the Research Landscape. In: *Tecnoscienza*, Band 4, 2013.

Ochs, Carsten und Löw, Martina: Un/Faire Informationspraktiken: Internet Privacy aus sozialwissenschaftlicher Perspektive. In: Buchmann, Johannes (Hg.) *Internet Privacy. Eine multidisziplinäre Bestandsaufnahme*. acatech – Deutsche Akademie der Technikwissenschaften, Darmstadt, 2012, S. 15–62.

OECD: The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines. OECD Digital Economy Papers 176, OECD, 2011.

Oetzel, Marie Caroline und Spiekermann, Sarah: Privacy-by-Design Through Systematic Privacy Impact Assessment – A Design Science Approach. In: *ECIS 2012*. 2012. Paper 160.

Offentlighets- och sekretesslagstiftningskommittén: *data och integritet*. Statens offentliga utredningar 1972:47. Stockholm, 1972.

Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. In: *UCLA Law Review*, Band 57: S. 1701–1777, 2010.

Ohm, Paul: Branding Privacy. In: *Minnesota Law Review*, Band 97: S. 907–989, 2013.

Ohm, Paul: Sensitive Information. In: *South California Law Review*, Band 88: S. 1125–1196, 2015.

Opfermann, Wilhelm: Informationsfreiheit als Voraussetzung für Meinungsfreiheit – Eine Problemskizze. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975, S. 21–25.

Otto, Paul N. und Antón, Annie I.: Addressing Legal Requirements in Requirements Engineering. In: *15th IEEE International Requirements Engineering Conference (RE 2007)*. 2007, S. 5–14.

Paaß, Gerhard und Wauschkuhn, Udo: *Datenzugang, Datenschutz und Anonymisierung: Analysepotential und Identifizierbarkeit von anonymisierten Individualdaten*, Band 148 von *Berichte der Gesellschaft für Mathematik und Datenverarbeitung*. R. Oldenbourg Verlag, München, Wien, 1985.

Packard, Vance: *The Naked Society.* David McKay Company, Inc., New York, 1964.

Pahlen-Brandt, Ingrid: Datenschutz braucht scharfe Instrumente: Beitrag zur Diskussion um „personenbezogene Daten“. In: *Datenschutz und Datensicherheit*, Band 32(1): S. 34–40, 2008.

Palen, Leysia und Dourish, Paul: Unpacking „Privacy“ for a Networked World. In: *Proceedings of the SIGCHI conference on Human factors in computing systems.* ACM, 2003, S. 129–136.

Palley, Michael A.: Security of Statistical Databases – Compromise through Attribute Correlational Modeling. In: *Proceedings of the Second International Conference on Data Engineering.* IEEE Computer Society, Washington, DC, USA, 1986, S. 67–74.

Parent, W. A.: Privacy, Morality, and the Law. In: *Philosophy & Public Affairs*, Band 12(4): S. 269–288, 1983.

Parsons, Carole: Computers and the International Flow of Information. In: *Computer Networks*, Band 3: S. 171–173, 1979.

Parsons, Talcott: *The Social System.* Routledge, London, 1951.

Pasquale, Frank: *The Black Box Society: The Secret Algorthms That Control Money and Information.* Harvard University Press, Cambridge, MA, 2015.

Patrick, Andrew S. und Kenny, Steve: From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. In: Dingledine, Roger (Hg.) *Privacy Enhancing Technologies 2003.* Springer, Berlin, Heidelberg, 2003, Band 2760 von *Lecture Notes in Computer Science*, S. 107–124.

Pennock, J. Roland und Chapman, John W. (Hg.): *Privacy*, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy.* Atherton Press, New York, 1971.

Peschek, Max und Steinmüller, Wilhelm: *Informatik und Gesellschaft*, Spektrum Akademischer Verlag, Heidelberg, Berlin, Oxford, Kapitel Datenschutz als Gestaltungsanforderung, S. 267–274. 1995.

Petersen, H. E. und Turn, Rein: System implications of information privacy. In: *Proceedings of the April 18-20, 1967, spring joint computer conference.* ACM, New York, NY, USA, 1967, AFIPS '67 (Spring), S. 291–300.

Petersen, Jens: *Das Bankgeheimnis zwischen Individualschutz und Institutionsschutz.* Mohr Siebeck, Tübingen, 2005.

Petersen, Stefanie: *Grenzen des Verrechtlichungsgebotes im Datenschutz.* LIT Verlag, Münster, 2000. Zugleich: Dissertation, Universität Hamburg.

Petri, Thomas B.: Datenschutz und Privatwirtschaft. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 221–237. 2004.

Petri, Thomas B.: Das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung“. In: *Datenschutz und Datensicherheit*, Band 32(7): S. 443–448, 2008.

Petronio, Sandra Sporbert: *Boundaries of Privacy.* State University of New York Press, Albany, New York, 2002.

Pettersson, John Sören, Fischer-Hübner, Simone und Bergmann, Mike: Outlining ‚Data Track ‘: Privacy-friendly Data Maintenance for End-users. In: Wojtkowski, Wita, Wojtkowski, W. Gregory, Zupancic, Joze, Magyar, Gabor und Knapp, Gabor (Hg.) *Advances in Information Systems Development*. 2006, Band 2, S. 215–226.

Pfitzmann, Andreas: Ein Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes in Bildschirmtext-ähnlichen Neuen Medien. In: Kupka, Ingbert (Hg.) *GI – 13. Jahrestagung*. Gesellschaft für Informatik, Springer, Berlin, Heidelberg, New York, 1983, Band 73 von *Informatik-Fachberichte*, S. 411–418.

Pfitzmann, Andreas: Technischer Datenschutz in dienstintegrierenden Digitalnetzen – Problemanalyse, Lösungsansätze und eine angepaßte Systemstruktur. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 96–112. 1985.

Pfitzmann, Andreas: *Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz*, Band 234 von *Informatik-Fachberichte*. Springer, Berlin, Heidelberg, New York, 1990.

Pfitzmann, Andreas: Möglichkeiten und Grenzen von Anonymität. In: Sokol, Bettina (Hg.) *Datenschutz und Anonymität*, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Düsseldorf, S. 9–37. 2000.

Pfitzmann, Andreas und Köhntopp, Marit: Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology. In: Federrath, Hannes (Hg.) *Designing Privacy Enhancing Technologie*. Springer, 2001, Band 2009 von *Lecture Notes in Computer Science*, S. 1–9.

Pfitzmann, Andreas, Pfitzmann, Birgit und Waidner, Michael: Technischer Datenschutz in dienstintegrierenden Digitalnetzen – Warum und wie? In: *Datenschutz und Datensicherung*, Band 10(3): S. 178–191, 1986.

Phillips, David J.: Cryptography, secrets, and the structuring of trust. In: Agre, Philip E. und Rotenberg, Marc (Hg.) *Technology and privacy: the new landscape*, MIT Press, Cambridge, MA, USA, S. 243–276. 1997.

Phillips, David J.: The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies. In: *arXiv preprint cs/0109098*, 2001.

Phillips, David J.: Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. In: *New Media & Society*, Band 6(6): S. 691–706, 2004.

Podlech, Adalbert: Rechtskybernetik – Eine juristische Disziplin der Zukunft. In: Erdsiek, Gerhard (Hg.) *Juristen-Jahrbuch*, Verlag Dr. Otto Schmidt KG, Köln-Marienburg, Band 10, S. 157–170. 1969.

Podlech, Adalbert: Verfassungsrechtliche Probleme öffentlicher Datenbanken. In: *Die Öffentliche Verwaltung*, Band 23(13–14): S. 473–475, 1970.

Podlech, Adalbert: Verfassungsrechtliche Probleme öffentlicher Informationssysteme. In: *Datenverarbeitung im Recht*, Band 1: S. 149–169, 1972.

Podlech, Adalbert: *Datenschutz im Bereich der öffentlichen Verwaltung*. Beiheft 1, Datenverarbeitung im Recht (DVR). J. Schweitzer Verlag, Berlin, 1973a.

Podlech, Adalbert: Prinzipien des Datenschutzes in der öffentlichen Verwaltung. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 3–13. 1973b.

Podlech, Adalbert: Datenschutz und das Verfassungsrecht. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975a, S. 27–33.

Podlech, Adalbert: Verfassung und Datenschutz. In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation*. Deutsche Verlags-Anstalt, Stuttgart, 1975b, S. 72–77.

Podlech, Adalbert: Aufgaben und Problematik des Datenschutzes. In: *Datenverarbeitung im Recht*, Band 5: S. 23–39, 1976a.

Podlech, Adalbert: Die Trennung von politischer, technischer und fachlicher Verantwortung in EDV-unterstützten Informationssystemen. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 207–216. 1976b.

Podlech, Adalbert: Gesellschaftstheoretische Grundlage des Datenschutzes. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 311–326. 1976c.

Podlech, Adalbert: Information – Modell – Abbildung – Eine Skizze. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 21–24. 1976d.

Podlech, Adalbert: Das Recht auf Privatheit. In: Perels, Joachim (Hg.) *Grundrechte als Fundament der Demokratie*, Suhrkamp Verlag, Frankfurt am Main, S. 50–68. 1979.

Podlech, Adalbert: Individualdatenschutz – Systemdatenschutz. In: Brückner, Klaus und Dalichau, Gerhard (Hg.) *Beiträge zum Sozialrecht – Festgabe für Grüner*, Verlag R. S. Schulz, Percha, S. 451–462. 1982.

Podlech, Adalbert: Ausgewählte Fragen zum Vertrauensärztlichen Dienst aus informationsrechtlicher Sicht. In: *Der Vertrauensärztliche Dienst in der Entwicklung*. Gesellschaft für Strahlen- und Umweltforschung mbH, Gesellschaft für Strahlen- und Umweltforschung mbH, München, 1983, S. 185–382.

Podlech, Adalbert: Die Begrenzung staatlicher Informationsverarbeitung durch die Verfassung angesichts der Möglichkeit unbegrenzter Informationsverarbeitung mittels der Technik. In: *Leviathan*, (1): S. 85–98, 1984.

Podlech, Adalbert: Unter welchen Bedingungen sind neue Informationssysteme gesellschaftlich akzeptabel? In: Steinmüller, Wilhelm (Hg.) *Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft*, Fischer Taschenbuch Verlag, Frankfurt am Main, S. 118–126. 1988.

Podlech, Adalbert: Die Transformation des für Informationssysteme geltenden Informationsrechts in die Informationssysteme steuerndes Systemrecht. In: *Datenschutz als Anforderung an die Systementwicklung*, Westdeutscher Verlag. 1990.

Pohle, Jörg: Ad fontes! – Neu nachdenken über Datenschutz. 2011. URL `http://waste.informatik.hu-berlin.de/~pohle/papers/AdFontes_20110902.pdf`.

Pohle, Jörg: Social Networks, Functional Differentiation of Society, and Data Protection. In: *arXiv preprint arXiv:1206.3027*, 2012.

Pohle, Jörg: Die immer noch aktuellen Grundfragen des Datenschutzes. In: Garstka, Hansjürgen und Coy, Wolfgang (Hg.) *Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis*. Humboldt-Universität zu Berlin, Hermann von Helmholtz-Zentrum für Kulturtechnik, Berlin, 2014a, S. 45–58. URL `http://nbn-resolving.de/urn:nbn:de:kobv:11-100217316`.

Pohle, Jörg: Kausalitäten, Korrelationen und Datenschutzrecht. In: Pohle, Jörg und Knaut, Andrea (Hg.) *Fundationes I: Geschichte und Theorie des Datenschutzes.* Monsenstein und Vannerdat, Münster, 2014b, S. 85–105.

Pohle, Jörg: Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens. In: *FIfF Kommunikation*, Band 32: S. 41–44, 2015a.

Pohle, Jörg: Zweckbindung revisited. In: *Datenschutz Nachrichten*, Band 38(3): S. 141–145, 2015b.

Pohle, Jörg: Die kategoriale Trennung zwischen »öffentlich« und »privat« ist durch die Digitalisierung aller Lebensbereiche überholt – Über einen bislang ignorierten Paradigmenwechsel in der Datenschutzdebatte. In: Plöse, Michael, Fritsche, Thomas, Kuhn, Michael und Lüders, Sven (Hg.) *»Worüber reden wir eigentlich?« Festgabe für Rosemarie Will.* Humanistische Union, Berlin, 2016a, S. 612–625.

Pohle, Jörg: PERSONAL DATA NOT FOUND: Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz. In: *Datenschutz Nachrichten*, Band 39(1): S. 14–19, 2016b.

Pohle, Jörg: Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen. In: *Mediale Kontrolle unter Beobachtung*, Band 5(1), 2016c.

Pohle, Jörg und Knaut, Andrea (Hg.): *Fundationes I: Geschichte und Theorie des Datenschutzes.* Monsenstein und Vannerdat, Münster, 2014.

Posner, Richard A.: An Economic Theory of Privacy. In: *AEI Journal on Government and Society*, S. 19–26, 1978a.

Posner, Richard A.: The Right to Privacy. In: *Georgia Law Review*, Band 12(3): S. 393–422, 1978b.

Posner, Richard A.: The Economics of Privacy. In: *The American Economic Review*, Band 71(2): S. 405–409, 1981.

Posner, Richard A.: Our Domestic Intelligence Crisis. In: *The Washington Post*, 2005. 21.12.2005.

Post, Robert C.: The Social Foundations of Privacy: Community and Self in the Common Law Tort. In: *California Law Review*, Band 77(5): S. 957–1010, 1989.

Post, Robert C.: Three Concepts of Privacy. In: *Georgetown Law Journal*, Band 89: S. 2087–2098, 2000.

Preisendörfer, Peter: *Organisationssoziologie: Grundlagen, Theorien und Problemstellungen.* VS Verlag für Sozialwissenschaften, Wiesbaden, 2008.

Privacy Protection Study Commission: *Personal privacy in an information society.* Privacy Protection Study Commission, Washington, D.C., 1977.

Probst, Thomas: Generische Schutzmaßnahmen für Datenschutz-Schutzziele. In: *Datenschutz und Datensicherheit*, Band 36(6): S. 439–444, 2012.

Prosser, William L.: Privacy. In: *California Law Review*, Band 48(3): S. 383–423, 1960.

Purtova, Nadezhda: Property rights in personal data: Learning from the American discourse. In: *Computer Law & Security Review*, Band 25(6): S. 507–521, 2009.

Raab, Charles D. und Bennett, Colin J.: Taking the measure of privacy: can data protection be evaluated? In: *International Review of Administrative Sciences*, Band 62(4): S. 535–556, 1996.

Raab, Charles D. und Bennett, Colin J.: The Distribution of Privacy Risks: Who Needs Protection? In: *The Information Society*, Band 14(4): S. 263–274, 1998.

Rachels, James: Why Privacy Is Important. In: *Philosophy & Public Affairs*, Band 4(4): S. 323–333, 1975.

Rachor, Frederik: Datenschutz und Richtervorbehalt. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 171–185. 2004.

Radin, Tara J.: The Privacy Paradox: E-Commerce and Personal Information on the Internet. In: *Business and Professional Ethics Journal*, Band 20(3 & 4): S. 145–170, 2001.

Raigrodski, Dana: Property, Privacy and Power: Rethinking the Fourth Amendment in the Wake of US v. Jones. In: *Boston University Public Interest Law Journal*, Band 22(1): S. 67–128, 2013.

Rammert, Werner: *Technik – Handeln – Wissen: Zu einer pragmatistischen Technik- und Sozialtheorie.* VS Verlag für Sozialwissenschaften, Wiesbaden, 2007.

Rannenberg, Kai: Datenschutz als Innovationsmotor statt als Technikfeind. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 190–205. 1998.

Rannenberg, Kai, Pfitzmann, Andreas und Müller, Günter: Sicherheit, insbesondere mehrseitige IT-Sicherheit. In: *Informationstechnik und technische Informatik*, Band 38: S. 7–10, 1996.

Rave, Dieter: Datenschutzprobleme am Beispiel des Gesundheitswesens. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 279–287. 1973.

Rave, Dieter: Ziele und Interessenlagen bei der Errichtung von Informationszentren in der öffentlichen Verwaltung. In: Schmitz, P. (Hg.) *Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung.* Gesellschaft für Informatik, Fachausschuß 8 „Methoden der Informatik für spezielle Anwendungen", Springer, Berlin, Heidelberg, New York, 1974, Band 9 von *Lecture Notes in Computer Science*, S. 116–123.

Raynes-Goldie, Katherine Sarah: Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. In: *First Monday*, Band 15(1), 2010. URL `http://www.firstmonday.dk/ojs/index.php/fm/article/view/2775`.

Raynes-Goldie, Katherine Sarah: *Privacy in the age of Facebook: Discourse, architecture, consequences.* Dissertation, Curtin University, Faculty of Humanities, Department of Internet Studies, 2012. URL `http://espace.library.curtin.edu.au/R?func=dbin-jump-full&local_base=gen01-era02&object_id=187731`.

Regan, Priscilla M.: Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations. In: *Journal of Public Policy*, Band 4(1): S. 19–38, 1984.

Regan, Priscilla M.: From Paper Dossiers to Electronic Dossiers: Gaps in the Privacy Act of 1974. In: *Information Technology & People*, Band 4(3): S. 279–296, 1988.

Regan, Priscilla M.: *Legislating Privacy.* The University of North Carolina Press, Chapel Hill, 1995.

Regan, Priscilla M.: Response to Bennett: Also in defence of privacy. In: *Surveillance & Society*, Band 8(4): S. 497–499, 2011.

Reh, Hans-Joachim: *Gegenstand und Aufgabe des Datenschutzes in der öffentlichen Verwaltung.* Nummer Heft 2 in Beiträge zum Datenschutz. Der Hessische Datenschutzbeauftragte, Wiesbaden, 1974.

Rehak, Rainer: *Angezapft: Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung*. Monsenstein und Vannerdat, Münster, 2014.

Reidenberg, Joel R.: Lex Informatica: The Formulation of Information Policy Rules Through Technology. In: *Texas Law Review*, Band 76(3): S. 553–584, 1998.

Reidenberg, Joel R.: Privacy Protection and the Interdependence of Law, Technology and Self-Regulation. In: *23rd International Conference of Data Protection Commissioners*. 2001.

Reidenberg, Joel R.: The Data Surveillance State in the US and Europe. Legal Studies Research Paper 2349269, Fordham University, School of Law, New York, 2013.

Richards, Neil M. und Solove, Daniel J.: Prosser's Privacy Law: A Mixed Legacy. In: *California Law Review*, Band 98: S. 1887–1924, 2010.

Rieger, Frank und Kurz, Constanze: Was der BND wirklich will. In: *Frankfurter Allgemeine Zeitung*, 2014. 17.11.2014, URL `http://www.faz.net/-hur-7wdtu`.

Riese, Cornelius: *Industrialisierung von Banken*. Deutscher Universitäts-Verlag, Wiesbaden, 2006.

Riesman, David, Glazer, Nathan und Denney, Reuel: *The Lonely Crowd*. Yale University Press, 1950. Nachdruck von 1953 durch Doubleday Anchor Books, Garden City, New York.

Rihaczek, Karl: Datenschutz im Wandel. In: *Datenschutz und Datensicherung*, Band 4(4): S. 228–231, 1980.

Rihaczek, Karl: Datenmißbrauch: Verhindern besser als verbieten. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 229–236. 1985.

Rivest, Ronald L., Adleman, Len und Dertouzos, Michael L.: On Data Banks and Privacy Homomorphisms. In: *Foundations of secure computation*, S. 169–177, 1978.

Robinson, John: The Snowden Disconnect: When the Ends Justify the Means. In: *SSRN*, 2014. URL `https://ssrn.com/abstract=2427412`.

Roessler, Thomas: Vermeidung von Spuren im Netz. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 205–213. 2000.

Ronge, Volker: Datendurst und Datenschutz. In: *Kursbuch*, Band 66: S. 108–128, 1981.

Rooms, Peter und Dexter, John: Problems of Data Protection Law for Private Multinational Communication Networks. In: *Computer Networks*, Band 3: S. 205–214, 1979.

Rosen, Jeffrey: The Purposes of Privacy: A Response. In: *Georgetown Law Journal*, Band 89: S. 2117–2137, 2000a.

Rosen, Jeffrey: *The Unwanted Gaze: The Destruction of Privacy in America*. Random House, New York, 2000b.

Rosen, Jeffrey: Out of Context: The Purposes of Privacy. In: *Social Research*, Band 68(1): S. 209–220, 2001.

Rossnagel, Heiko: The Market Failure of Anonymity Services. In: Samarati, P. (Hg.) *WISTP 2010*. Springer, Berlin, 2010, Band 6033 von *Lecture Notes in Computer Science*, S. 340–354.

Rost, Martin: Zur gesellschaftlichen Funktion des Datenschutzes. In: *juridikum*, (1): S. 49–51, 2002.

Rost, Martin: Zur gesellschaftlichen Funktion von Anonymität. In: *Datenschutz und Datensicherheit*, Band 27(3): S. 155–158, 2003a.

Rost, Martin: Über die Funktionalität von Anonymität für die bürgerliche Gesellschaft. In: Bäumler, Helmut und von Mutius, Albert (Hg.) *Anonymität im Internet. Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts*, Springer Fachmedien, Wiesbaden, S. 62–73. 2003b.

Rost, Martin: Verkettbarkeit als Grundbegriff des Datenschutzes? Identitätsmanagement soziologisch betrachtet. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 315–334. 2004.

Rost, Martin: Gegen große Feuer helfen große Gegenfeuer – Datenschutz als Wächter funktionaler Differenzierung. In: *vorgänge*, (4): S. 15–26, 2008a.

Rost, Martin: User-Centric-Workflow für den EAP. In: *Datenschutz und Datensicherheit*, Band 32(7): S. 439–442, 2008b.

Rost, Martin: Interview mit Paul J. Müller. 2012a. Interviews zur Geschichte und Programmatik des Datenschutzes in Deutschland, URL `https://www.datenschutzzentrum.de/interviews/mueller/`.

Rost, Martin: Standardisierte Datenschutzmodellierung. In: *Datenschutz und Datensicherheit*, Band 36(6): S. 433–438, 2012b.

Rost, Martin: Datenschutzmanagementsystem. In: *Datenschutz und Datensicherheit*, Band 37(5): S. 295–300, 2013a.

Rost, Martin: Zur Soziologie des Datenschutzes. In: *Datenschutz und Datensicherheit*, Band 37(2): S. 85–91, 2013b.

Rost, Martin: Neun Thesen zum Datenschutz. In: Pohle, Jörg und Knaut, Andrea (Hg.) *Fundationes I: Geschichte und Theorie des Datenschutzes*. Monsenstein und Vannerdat, Münster, 2014a, S. 37–44.

Rost, Martin: Was meint eigentlich „Datenschutz“? In: *Der Landkreis*, (3): S. 72–74, 2014b.

Rost, Martin: Lässt sich Datenschutz durch Ethik ersetzen? 2016. URL `http://blog.maroki.de/2016/05/laesst-sich-datenschutz-durch-ethik-ersetzen/`.

Rost, Martin und Bock, Kirsten: Impact Assessment im Lichte des Standard-Datenschutzmodells. In: *Datenschutz und Datensicherheit*, Band 36(10): S. 743–747, 2012.

Rost, Martin und Krasemann, Henry: Interview mit Adalbert Podlech. 2008. Interviews zur Geschichte und Programmatik des Datenschutzes in Deutschland, URL `https://www.datenschutzzentrum.de/interviews/podlech/`.

Rost, Martin und Krasemann, Henry: Interview mit Prof. Dr. Wilhelm Steinmüller. 2009. Interviews zur Geschichte und Programmatik des Datenschutzes in Deutschland, URL `https://www.datenschutzzentrum.de/interviews/steinmueller/`.

Rost, Martin und Meints, Martin: Authentisierung in Sozialsystemen – Identitytheft strukturell betrachtet. In: *Datenschutz und Datensicherheit*, Band 29(4): S. 216–218, 2005.

Rost, Martin und Pfitzmann, Andreas: Datenschutz-Schutzziele – revisited. In: *Datenschutz und Datensicherheit*, Band 33(6): S. 353–358, 2009.

Rost, Martin und Storf, Katalin: Zur Konditionierung von Technik und Recht mittels Schutzzielen. In: Horbach, Matthias (Hg.) *Informatik 2013 : Informatik angepasst an Mensch, Organisation und Umwelt*. Gesellschaft für Informatik, Bonn, 2013, Band 220 von *Lecture Notes in Informatics*, S. 2149–2166.

Rotenberg, Marc: Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get). In: *Stanford Technology Law Review*, Band 1, 2001. URL `http://stlr.stanford.edu/pdf/rotenberg-fair-info-practices.pdf`.

Rouvroy, Antoinette: Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. In: *Studies in Ethics, Law, and Technology*, Band 2(1), 2008. Article 3, URL `https://doi.org/10.2202/1941-6008.1001`.

Rouvroy, Antoinette: The end(s) of critique: data behaviourism versus due process. In: Hildebrandt, Mireille und de Vries, Katja (Hg.) *Privacy, Due Process and the Computational Turn*. Routledge, Abingdon, 2013, S. 143–167.

Roßnagel, Alexander: Sozialverträglichkeit von Computern – rechtlich gesehen. In: Rammert, Werner und Bechmann, Gotthard (Hg.) *Technik und Gesellschaft, Jahrbuch 5*. Campus Verlag, Frankfurt am Main, New York, 1989a, S. 125–147.

Roßnagel, Alexander: Verfassungsverträglichkeit – Ein Kriterium der Technikbewertung. In: Schaaf, Jutta (Hg.) *Die Würde des Menschen ist unverNETZbar*. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., FIfF, Frankfurt am Main, 1989b, S. 238–254.

Roßnagel, Alexander: Freiheit durch Systemgestaltung. In: Nickel, Egbert, Roßnagel, Alexander und Schlink, Bernhard (Hg.) *Die Freiheit und die Macht: Wissenschaft im Ernstfall; Festschrift für Adalbert Podlech*, Nomos Verlagsgesellschaft, Baden-Baden, S. 227–246. 1994.

Roßnagel, Alexander: Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger. In: *Zeitschrift für Rechtspolitik*, (1): S. 26–30, 1997.

Roßnagel, Alexander: Datenschutz-Audit – ein neues Instrument des Datenschutzes. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 65–80. 1998.

Roßnagel, Alexander: Datenschutz-Audit. In: Sokol, Bettina (Hg.) *Neue Instrumente im Datenschutz*, Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Düsseldorf, S. 41–63. 1999.

Roßnagel, Alexander: Datenschutz 2015 – in einer Welt des Ubiquitous Computing. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 335–351. 2004.

Roßnagel, Alexander und Bizer, Johann: *Multimediadienste und Datenschutz*. Akademie für Technikfolgenabschätzung in Baden-Württemberg, Stuttgart, 1995.

Roßnagel, Alexander, Pfitzmann, Andreas und Garstka, Hansjürgen: Modernisierung des Datenschutzrechts. Gutachten, Bundesministerium des Innern, 2001.

Roßnagel, Alexander, Wedde, Peter, Hammer, Volker und Pordesch, Ulrich: *Die Verletzlichkeit der 'Informationsgesellschaft'*, Band 5 von *Sozialverträgliche Technikgestaltung*. Westdeutscher Verlag, Opladen, zweite Auflage, 1990a.

Roßnagel, Alexander, Wedde, Peter, Hammer, Volker und Pordesch, Ulrich: *Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik*, Band 8 von *Sozialverträgliche Technikgestaltung*. Westdeutscher Verlag, Opladen, 1990b.

Rubenfeld, Jed: The Right of Privacy. In: *Harvard Law Review*, Band 102(4): S. 737–807, 1989.

Rubin, Michael Rogers: The Computer and Personal Privacy, Part I: The Individual Under Assault. In: *Library Hi Tech*, Band 5(1): S. 23–31, 1987.

Rubin, Michael Rogers: The Computer and Personal Privacy, Part II: The Emerging Worldwide Response to the Threat to Privacy from Computer Databases. In: *Library Hi Tech*, Band 6(1): S. 87–96, 1988.

Rubin, Michael Rogers: The Computer and Personal Privacy, Part III: The Regulation of Computer Records in the United States. In: *Library Hi Tech*, Band 7(3): S. 11–21, 1989.

Rubinstein, Ira S., Lee, Ronald D. und Schwartz, Paul M.: Data mining and Internet profiling: Emerging regulatory and technological approaches. In: *The University of Chicago Law Review*, Band 75(1): S. 261–285, 2008.

Ruebhausen, Oscar M. und Brim, Orville G., Jr.: Privacy and Behavioral Research. In: *Columbia Law Review*, Band 65(7): S. 1184–1211, 1965.

Rule, James B.: *Private Lives and Public Surveillance.* Allen Lane, London, 1973.

Rule, James B.: 1984–The Ingredients of Totalitarianism. In: Howe, Irving (Hg.) *1984 Revisited*, Harper & Row, New York, Kapitel 11, S. 166–179. 1983.

Rule, James B.: Introduction. In: Rule, James B. und Greenleaf, Graham (Hg.) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, S. 1–14. 2008.

Rule, James B. und Brantley, Peter: Computerized Surveillance in the Workplace: Forms and Distributions. In: *Sociological Forum*, Band 7(3): S. 405–423, 1992.

Rule, James B., McAdam, Douglas, Stearns, Linda und Uglow, David: *The Politics of Privacy.* Elsevier, New York, 1980.

Rustad, Michael L. und Kulevska, Sanna: Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow. In: *Harvard Journal of Law and Technology*, Band 28(2): S. 349–417, 2015.

Rössler, Beate: *Der Wert des Privaten.* Suhrkamp Verlag, Frankfurt am Main, 2001.

Rötzer, Florian: Das Recht auf Anonymität. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 27–34. 2000.

Rüpke, Giselher: *Der verfassungsrechtliche Schutz der Privatheit. Zugleich ein Versuch pragmatischen Grundrechtsverständnisses.* Nomos Verlagsgesellschaft, Baden-Baden, 1976.

Samarati, Pierangela und Sweeney, Latanya: Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement through Generalization and Suppression. In: *Proceedings of the IEEE Symposium on Research in Security and Privacy (S&P)*. 1998.

Sasse, Christoph: *Sinn und Unsinn des Datenschutzes.* C. F. Müller Verlag, Karlsruhe und Heidelberg, 1976.

Schallaböck, Jan: Datenschutzkontrolle durch Open-Source. In: *Datenschutz und Datensicherheit*, Band 33(3): S. 161–166, 2009.

Schartum, Dag Wiese: Privacy Enhancing Employment of ICT: Empowering and Assisting Data Subjects. In: *International Review of Law, Computers & Technology*, Band 15(2): S. 157–169, 2001.

Schelsky, Helmut: *Die sozialen Folgen der Automatisierung.* Eugen Diederichs Verlag, Düsseldorf, Köln, 1957.

Schermer, Bart: The limits of privacy in automated profiling and data mining. In: *Computer Law & Security Review*, Band 27(1): S. 45–52, 2011.

Scheuch, Erwin K.: Datenschutz als Machtkontrolle. In: Dammann, Ulrich, Karhausen, Mark O., Müller, Paul J. und Steinmüller, Wilhelm (Hg.) *Datenbanken und Datenschutz*, Herder & Herder, Frankfurt am Main, S. 171–176. 1974.

Scheuch, Erwin K.: Die Weiterentwicklung des Datenschutzes als Problem der Sozialforschung. In: Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros (Hg.) *Datenzugang und Datenschutz*, Athenäum, Königstein/Ts., S. 252–275. 1980.

Schild, Hans-Hermann und Tinnefeld, Marie-Theres: Datenschutz in der Union – Gelungene oder missglückte Gesetzentwürfe? In: *Datenschutz und Datensicherheit*, Band 36(5): S. 312–317, 2012.

Schiller, Herbert I.: Computer Systems: Power for Whom and for What? In: *Journal of Communication*, Band 28(4): S. 184–193, 1978.

Schimmel, Wolfgang und Steinmüller, Wilhelm: Rechtspolitische Problemstellung des Datenschutzes. In: Dammann, Ulrich, Karhausen, Mark O., Müller, Paul J. und Steinmüller, Wilhelm (Hg.) *Datenbanken und Datenschutz*, Herder & Herder, Frankfurt am Main, S. 111–169. 1974.

Schinzel, Britta: Algorithmen sind nicht schuld, aber wer oder was ist es dann? In: *FIfF Kommunikation*, Band 34(2): S. 5–9, 2017.

Schlink, Bernhard: Der Bürger als Datenobjekt. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 155–172. 1973.

Schlink, Bernhard: Das Recht der informationellen Selbstbestimmung. In: *Der Staat*, S. 233–250, 1986.

Schlörer, Jan: Anfragenverbote als Dialogsicherung für statistische Datenbanken – Voraussetzungen und Schwierigkeiten. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 155–168. 1976.

Schlörer, Jan: Anonymisierung von Mikrodaten in der Forschung: Technische Aspekte. In: Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros (Hg.) *Datenzugang und Datenschutz*, Athenäum, Königstein/Ts., S. 118–142. 1980.

Schmale, Wolfgang und Tinnefeld, Marie-Theres: „Der Bau“ von Kafka oder die (Staats)Trojaner-Architektur. In: *Datenschutz und Datensicherheit*, Band 36(6): S. 401–405, 2012.

Schmidt, Kjeld und Bannon, Liam: Taking CSCW seriously. In: *Computer Supported Cooperative Work (CSCW)*, Band 1(1): S. 7–40, 1992.

Schmidt, Walter: Die bedrohte Entscheidungsfreiheit. In: *Juristenzeitung*, Band 28(8): S. 241–250, 1974.

Schmidt, Werner: Zur Änderung des § 6 BDSG und der Anlage. In: *Datenschutz und Datensicherung*, Band 10(1): S. 5, 1986.

Schneider, Jochen: *Datenschutz – Datensicherung.* Heft 5 Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung. Siemens Aktiengesellschaft, München, 1971.

Schneider, Jochen: Technische Möglichkeiten des Datenschutzes. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 223–233. 1973.

Schneider, Jochen: Probleme der Implementierung von "Privacy" in Informationszentren. In: Schmitz, P. (Hg.) *Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung.* Gesellschaft für Informatik, Fachausschuß 8 „Methoden der Informatik für spezielle Anwendungen“, Springer, Berlin, Heidelberg, New York, 1974, Band 9 von *Lecture Notes in Computer Science*, S. 206–214.

Schneier, Bruce: Threat Modeling and Risk Assessment. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 214–229. 2000.

Schneier, Bruce: *Secrets and lies: digital security in a networked world.* Wiley Publishing, Indianapolis, 2004. Paperback Edition.

Schnepel, Johannes und Steinmüller, Wilhelm: Ziele informationstechnologischer Bildung. Ein Plädoyer gegen Programmierwahn und für soziale Beherrschung. In: Steinmüller, Wilhelm (Hg.) *Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft*, Fischer Taschenbuch Verlag, Frankfurt am Main, S. 179–191. 1988.

Schoeman, Ferdinand: *Philosophical Dimensions of Privacy: An Anthology.* Cambridge University Press, Cambridge, 1984a.

Schoeman, Ferdinand: Privacy: Philosophical Dimensions. In: *American Philosophical Quarterly*, Band 21(3): S. 199–213, 1984b.

Schoeman, Ferdinand: Privacy: Philosophical dimensions of the literature. In: *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, Cambridge. 1984c.

Schoeman, Ferdinand: *Privacy and social freedom.* Cambridge University Press, Cambridge, 1992.

Scholz, Renate: Datenschutz als Sozialverträglichkeitskriterium und als informationstechnisches Gestaltungsprinzip. In: *Datenschutz und Datensicherung*, Band 12(3): S. 117–123, 1988.

Schomerus, Rudolf: Datenschutz oder Datenverkehrsordnung? In: *Zeitschrift für Rechtspolitik*, S. 291–294, 1981.

Schrader, Hans-Hermann: Selbstdatenschutz: Effektive Wahrnehmung des Selbstbestimmungsrechts. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz“ – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 206–212. 1998.

Schrempf, Martin: *Datenschutz bei TEMEX: Risiken von Fernwirkdiensten und Möglichkeiten einer datenschutzgerechten Technikgestaltung*, Band 11. Vieweg, Braunschweig, 1990.

Schwan, Eggert: Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte. In: *Verwaltungsarchiv*, Band 66: S. 120–150, 1975a.

Schwan, Eggert: Rechtsschutz für den Bürger vor staatlicher Informationssammlung. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger.* Peter Hammer Verlag, Wuppertal, 1975b, S. 36–40.

Schwan, Eggert: Auf dem Weg zum Überwachungsstaat? Plädoyer für eine rechtsstaatliche Datenverarbeitung der Polizei. In: Hohmann, Harald (Hg.) *Freiheitssicherung durch Datenschutz.* Suhrkamp Verlag, Frankfurt am Main, 1987, S. 276–312.

Schwartz, Paul M.: The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. In: *The American Journal of Comparative Law*, Band 37(4): S. 675–701, 1989.

Schwartz, Paul M.: Data Processing and Government Administration: The Failure of the American Legal Response to the Computer. In: *Hastings Law Journal*, Band 43: S. 1321–1388, 1992.

Schwartz, Paul M.: Internet Privacy and the State. In: *Connecticut Law Review*, Band 32: S. 815–859, 1999a.

Schwartz, Paul M.: Privacy and Democracy in Cyberspace. In: *Vanderbilt Law Review*, Band 52: S. 1609–1702, 1999b.

Schwartz, Paul M.: Property, Privacy, and Personal Data. In: *Harvard Law Review*, Band 117: S. 2056–2128, 2003.

Schwartz, Paul M. und Peifer, Karl-Nikolaus: Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept? In: *California Law Review*, Band 98: S. 1925–1987, 2010.

Schwartz, Paul M. und Solove, Daniel J.: The PII Problem: Privacy and a New Concept of Personally Identifiable Information. In: *New York University Law Review*, Band 86: S. 1814–1894, 2011.

Schwartz, Paul M. und Treanor, William M.: The New Privacy. In: *Michigan Law Review*, Band 101: S. 2163–2184, 2003.

Schwenke, Matthias Christoph: *Individualisierung und Datenschutz*. Deutscher Universitäts-Verlag, Wiesbaden, 2006.

Seelos, Hans-Jürgen: *Informationssysteme und Datenschutz im Krankenhaus*, Band 14. Vieweg, Braunschweig, Wiesbaden, 1991.

Seidel, Ulrich: Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten. In: *Neue Juristische Wochenschrift*, S. 1581–1583, 1970.

Seidel, Ulrich: *Datenbanken und Persönlichkeitsrecht unter besonderer Berücksichtigung der amerikanischen Computer Privacy*. Verlag Dr. Otto Schmidt KG, Köln, 1972.

Seidel, Ulrich: Die durchlöcherte Privatsphäre. In: Krauch, Helmut (Hg.) *Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation*. Deutsche Verlags-Anstalt, Stuttgart, 1975, S. 38–47.

Seidel, Ulrich: Voraussetzungen und Gestaltungsgrundsätze „ordnungsgemäß wirkender Systeme". In: Kuhlen, Rainer (Hg.) *Koordination von Informationen*. Gesellschaft für Informatik, Springer, Berlin, Heidelberg, New York, 1984, Band 81 von *Informatik-Fachberichte*, S. 190–194.

Shannon, Claude E.: A Mathematical Theory of Communication. In: *The Bell System Technical Journal*, Band 27(3): S. 379–423, 1948.

Shattuck, John: Computer matching is a serious threat to individual rights. In: *Communications of the ACM*, Band 27(6): S. 538–541, 1984.

Shils, Edward: Privacy: Its Constitution and Vicissitudes. In: *Law and Contemporary Problems*, Band 31(2): S. 281–306, 1966.

Shoor, Emily: Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation. In: *Brooklyn Journal of International Law*, Band 39(1): S. 487–519, 2014.

Siena, Alberto, Mylopoulos, John, Perini, Anna und Susi, Angelo: The Nomos framework: Modelling Requirements Compliant with Laws. Technical Report TR-0209-SMSP, 2009.

Simitis, Spiros: *Automation in der Rechtsordnung – Möglichkeiten und Grenzen*. Verlag C. F. Müller, Karlsruhe, 1967.

Simitis, Spiros: *Informationskrise des Rechts und Datenverarbeitung*, Band 7 von *Recht – Justiz – Zeitgeschehen (RJZ)*. Verlag C. F. Müller, Karlsruhe, 1970.

Simitis, Spiros: Datenschutz – Notwendigkeit und Voraussetzung einer gesetzlichen Regelung. In: *Datenverarbeitung im Recht*, Band 2: S. 138–189, 1973.

Simitis, Spiros: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. In: *Neue Juristische Wochenschrift*, (8): S. 398–405, 1984.

Simitis, Spiros: Reicht unser Datenschutz angesichts der technischen Revolution? – Strategien zur Wahrung der Freiheitsrechte. In: von Schoeler, Andreas (Hg.) *Informationsgesellschaft oder Überwachungsstaat?*, Westdeutscher Verlag, Opladen, S. 21–41. 1986.

Simitis, Spiros: Reviewing Privacy in an Information Society. In: *University of Pennsylvania Law Review*, Band 135: S. 707–746, 1987.

Simitis, Spiros: „Sensitive Daten" – Zur Geschichte und Wirkung einer Fiktion. In: Brem, Ernst, Druey, Jean N., Kramer, Ernst A. und Schwander, Ivo (Hg.) *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini*, Stämpfli & Cie, Bern, S. 469–493. 1990.

Simitis, Spiros: Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz? In: *Neue Juristische Wochenschrift*, Band 50(5): S. 281–288, 1997.

Simitis, Spiros: Datenschutz – Rückschritt oder Neubeginn? In: *Neue Juristische Wochenschrift*, Band 51(34): S. 2473–2479, 1998.

Simitis, Spiros: Die Erosion des Datenschutzes. In: Sokol, Bettina (Hg.) *Neue Instrumente im Datenschutz*, Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Düsseldorf, S. 5–40. 1999.

Simitis, Spiros: Das Volkszählungsurteil oder der lange Weg zur Informationsaskese – (BVerfGE 65, 1). In: *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft*, Band 83: S. 359–375, 2000.

Simitis, Spiros: Datenschutz – eine notwendige Utopie. In: Kiesow, Rainer Maria, Ogorek, Regina und Simitis, Spiros (Hg.) *Summa. Dieter Simon zum 70. Geburtstag*, Vittorio Klostermann, Frankfurt am Main, S. 511–527. 2005.

Simitis, Spiros: Hat der Datenschutz noch eine Zukunft? In: *Recht der Datenverarbeitung*, Band 23(4): S. 143–153, 2007.

Simitis, Spiros: Privacy—An Endless Debate? In: *California Law Review*, Band 98: S. 1989–2005, 2010.

Simitis, Spiros (Hg.): *Bundesdatenschutzgesetz.* Nomos Verlagsgesellschaft, Baden-Baden, 7. Auflage, 2011.

Simon, Claus: Datenschutz im IT-Grundschutz. In: *Datenschutz und Datensicherheit*, Band 31(2): S. 87–90, 2007.

Simon, Herbert A.: The Architecture of Complexity. In: *Proceedings of the American Philosophical Society*, Band 106(6): S. 467–482, 1962.

Singelnstein, Tobias und Stolle, Peer: *Die Sicherheitsgesellschaft: Soziale Kontrolle im 21. Jahrhundert.* VS Verlag für Sozialwissenschaften, Wiesbaden, dritte Auflage, 2012.

Smith, H. Jeff, Dinev, Tamara und Xu, Heng: Information Privacy Research: An Interdisciplinary Review. In: *MIS Quarterly*, Band 35(4): S. 989–1015, 2011.

Sofsky, Wolfgang und Paris, Rainer: *Figurationen sozialer Macht – Autorität, Stellvertretung, Koalition.* Suhrkamp Verlag, Frankfurt am Main, 1994.

Sokol, Bettina: Eröffnung. In: Sokol, Bettina (Hg.) *Neue Instrumente im Datenschutz*, Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Düsseldorf, S. 3–4. 1999.

Sokol, Bettina (Hg.): *Der gläserne Mensch – DNA-Analysen, eine Herausforderung an den Datenschutz.* Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Düsseldorf, 2003.

Solove, Daniel J.: Privacy and Power: Computer Databases and Metaphors for Information Privacy. In: *Stanford Law Review*, Band 53(6): S. 1393–1462, 2001.

Solove, Daniel J.: Conceptualizing Privacy. In: *California Law Review*, Band 90(4): S. 1087–1155, 2002.

Solove, Daniel J.: *The Digital Person: Technology and Privacy in the Information Age*. New York University Press, New York, 2004.

Solove, Daniel J.: A Taxonomy of Privacy. In: *University of Pennsylvania Law Review*, Band 154(3): S. 477–560, 2006.

Solove, Daniel J.: „I've Got Nothing to Hide" and Other Misunderstandings of Privacy. In: *San Diego Law Review*, Band 44: S. 745–772, 2007.

Solove, Daniel J.: *Understanding Privacy*. Harvard University Press, Cambridge, 2009. Paperback Edition.

Solove, Daniel J.: Privacy Self-Management and the Consent Dilemma. In: *Harvard Law Review*, Band 126: S. 1880–1903, 2013.

Sommer, Dieter, Casassa Mont, Mario und Pearson, Siani: PRIME Architecture V3. Deliverable D14.2.d, PRIME, 2008.

Spiekermann, Sarah und Cranor, Lorrie Faith: Engineering Privacy. In: *IEEE Trans. Softw. Eng.*, Band 35(1): S. 67–82, 2009.

Spiekermann, Sarah, Grossklags, Jens und Berendt, Bettina: E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior. In: *Proceedings of the 3rd ACM conference on Electronic Commerce*. 2001, S. 38–47.

Spies, Peter Paul (Hg.): *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Band 113 von *Informatik-Fachberichte*. Springer-Verlag, Berlin, 1985a.

Spies, Peter Paul: Datenschutz und Datensicherung im Wandel der Informationstechnologien. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 1–25. 1985b.

Stadlen, Godfrey: Survey of National Data Protection Legislation. In: *Computer Networks*, Band 3: S. 174–186, 1979.

Stahl, Titus: Indiscriminate mass surveillance and the public sphere. In: *Ethics and Information Technology*, Band 18(1): S. 33–39, 2016.

Stalder, Felix: Privacy is not the antidote to surveillance. In: *Surveillance & Society*, Band 1(1): S. 120–124, 2002a.

Stalder, Felix: The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy. In: *Sociological Research Online*, Band 7(2), 2002b. URL `http://www.socresonline.org.uk/7/2/stalder.html`.

Stalder, Felix: Autonomy beyond privacy? A rejoinder to Bennett. In: *Surveillance & Society*, Band 8(4): S. 508–512, 2011.

Stanton, Jeffrey M. und Stam, Kathryn R.: Information Technology, Privacy, and Power within Organizations: a view from Boundary Theory and Social Exchange Perspectives. In: *Surveillance & Society*, Band 1(2): S. 152–190, 2003.

Steinbock, Daniel J.: Data Matching, Data Mining, and Due Process. In: *Georgia Law Review*, Band 40(1): S. 1–84, 2005.

Steinbuch, Karl: Informationstechnik und Liberalität. In: *Informationstechnik und Liberalität*. Ludwig-Erhard-Stiftung e.V. Bonn, Gustav Fischer Verlag, Stuttgart, 1980, S. 3–21.

Steinbuch, Karl und Wacker, Herbert: Überlegungen zu technischen Möglichkeiten des Datenschutzes im Hinblick auf ein Bundesdatenschutzgesetz. Gutachten, Bundesministerium des Innern, 1972. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 3.

Steinmüller, Wilhelm: *EDV und Recht – Einführung in die Rechtsinformatik*. J. Schweitzer Verlag, Berlin, 1970.

Steinmüller, Wilhelm: Allgemeine Grundsätze zur rechtlichen Regelung des Datenschutzes. In: Schneider, Jochen (Hg.) *Datenschutz – Datensicherung*, Siemens Aktiengesellschaft, München, Heft 5 Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung, Kapitel 3, S. 13–17. 1971a.

Steinmüller, Wilhelm: Rechtsinformatik. Elektronische Datenverarbeitung und Recht. In: *Juristische Rundschau*, (1): S. 1–9, 1971b.

Steinmüller, Wilhelm: Rechtspolitische Bemerkungen zum geplanten staatlichen Informationssystem. In: Würtenberger, Thomas (Hg.) *Rechtsphilosophie und Rechtspraxis. Referate auf der Tagung der Deutschen Sektion der Internationalen Vereinigung für Rechts- und Sozialphilosophie e.V. in Freibug i. Br. am 7. Oktober 1970*. Vittorio Klostermann, Frankfurt am Main, 1971c, S. 81–87.

Steinmüller, Wilhelm: Gegenstand, Grundbegriffe und Systematik der Rechtsinformatik. Ansätze künftiger Theoriebildung. In: *Datenverarbeitung im Recht*, Band 1: S. 113–148, 1972a.

Steinmüller, Wilhelm: Stellenwert der EDV in der Öffentlichen Verwaltung und Prinzipien des Datenschutzrechts. In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 2(11): S. 453–462, 1972b.

Steinmüller, Wilhelm: Objektbereich „Verwaltungsautomation“ und Prinzipien des Datenschutzes. In: Kilian, Wolfgang, Lenk, Klaus und Steinmüller, Wilhelm (Hg.) *Datenschutz*, Athenäum-Verlag, Frankfurt am Main, Band 1 von *Beiträge zur juristischen Informatik*, S. 51–76. 1973.

Steinmüller, Wilhelm: Datenschutzrechtliche Anforderungen an die Organisation von Informationszentren. In: Schmitz, P. (Hg.) *Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung*. Gesellschaft für Informatik, Fachausschuß 8 „Methoden der Informatik für spezielle Anwendungen“, Springer, Berlin, Heidelberg, New York, 1974, Band 9 von *Lecture Notes in Computer Science*, S. 187–205.

Steinmüller, Wilhelm: Automationsunterstützte Informationssysteme in privaten und öffentlichen Verwaltungen. Bruchstücke einer alternativen Theorie des Datenzeitalters. In: *Leviathan*, Band 4(3): S. 508–543, 1975a.

Steinmüller, Wilhelm: Datenschutz als Teilaspekt gesellschaftlicher Informationskontrolle. In: Löchner, Gerhard und Steinmüller, Wilhelm (Hg.) *Datenschutz und Datensicherung*. Deutsche Sektion der Internationalen Juristen-Kommission, C. F. Müller Verlag, Karlsruhe, 1975b, Band 1 von *Rechtsstaat in der Bewährung*, S. 35–95.

Steinmüller, Wilhelm: Quo vadis, Computer? – Vermutungen über Alternativen künftiger sozioökonomischer Entwicklungen. In: Hoffmann, Gerd E., Tietze, Barbara und Podlech, Adalbert (Hg.) *Numerierte Bürger*. Peter Hammer Verlag, Wuppertal, 1975c, S. 139–147.

Steinmüller, Wilhelm: Einleitung. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. IX–XI. 1976a.

Steinmüller, Wilhelm (Hg.): *Informationsrecht und Informationspolitik*. Nummer 1 in Rechtstheorie und Informationsrecht. Oldenbourg Verlag, München, Wien, 1976b.

Steinmüller, Wilhelm: Informationsrecht und Informationspolitik. In: Steinmüller, Wilhelm (Hg.) *Informationsrecht und Informationspolitik*, Oldenbourg Verlag, München, Wien, Nummer 1 in Rechtstheorie und Informationsrecht, S. 1–20. 1976c.

Steinmüller, Wilhelm: Der aufhaltsame Aufstieg des Geheimbereichs. In: *Kursbuch*, Band 56: S. 169–198, 1979a.

Steinmüller, Wilhelm: Informationstechnologien und gesellschaftliche Macht: Zur Notwendigkeit einer informationspolitischen Gesamtkonzeption. In: *WSI Mitteilungen*, (8): S. 426–436, 1979b.

Steinmüller, Wilhelm: Legal Problems of Computer Networks: A Methodological Survey. In: *Computer Networks*, Band 3: S. 187–198, 1979c.

Steinmüller, Wilhelm: Übertragbarkeit herkömmlicher Datenschutzvorstellungen auf Breitbandkommunikation. In: Dette, Klaus, Kreibich, Rolf und Steinmüller, Wilhelm (Hg.) *Zweiweg-Kabelfernsehen und Datenschutz*. Institut für Zukunftsforschung, Minerva Publikation, München, 1979d, Band 1 von *Beiträge des Instituts für Zukunftsforschung*, S. 81–94. Dokumentation des Colloquiums vom 12. September 1978 „Zweiweg-Kabelfernsehen und Datenschutz“.

Steinmüller, Wilhelm: Ein organisationsunterstütztes Verfahren zur Anonymisierung von Forschungsdaten. In: Kaase, Max, Krupp, Hans-Jürgen, Pflanz, Manfred, Scheuch, Erwin K. und Simitis, Spiros (Hg.) *Datenzugang und Datenschutz*, Athenäum, Königstein/Ts., S. 111–117. 1980a.

Steinmüller, Wilhelm: Rationalisation and Modellification: Two Complementary Implications of Information Technologies. In: Lavington, Simon H. (Hg.) *Information Processing 80*. North-Holland, Amsterdam, 1980b, IFIP congress series, S. 853–861.

Steinmüller, Wilhelm: Soziale Auswirkungen und Gestaltungen der Informationstechnologie. In: *Informationstechnik und Liberalität*. Ludwig-Erhard-Stiftung e.V. Bonn, Gustav Fischer Verlag, Stuttgart, 1980c, S. 87–128.

Steinmüller, Wilhelm: Die Zweite industrielle Revolution hat eben begonnen – Über die Technisierung der geistigen Arbeit. In: *Kursbuch*, Band 66: S. 152–188, 1981.

Steinmüller, Wilhelm: Das Volkszählungsurteil des Bundesverfassungsgerichts. In: *Datenschutz und Datensicherung*, Band 8(2): S. 91–96, 1984.

Steinmüller, Wilhelm: *Informationstechnologien, Personalinformationssysteme und Handlungsmöglichkeiten der Betroffenen*. Schriftenreihe der Beratungsstelle für Informationstechnik-Folgen und -Alternativen (BIFA). Universität Bremen, Bremen, 1985a.

Steinmüller, Wilhelm: Soziale Beherrschbarkeit offener Netze. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 237–249. 1985b.

Steinmüller, Wilhelm: Betroffenenschutz bei offenen Netzen. In: Hohmann, Harald (Hg.) *Freiheitssicherung durch Datenschutz*. Suhrkamp Verlag, Frankfurt am Main, 1987, S. 62–84.

Steinmüller, Wilhelm: Demokratische und soziale Informationstechnologiepolitik. In: Steinmüller, Wilhelm (Hg.) *Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft*, Fischer Taschenbuch Verlag, Frankfurt am Main, S. 17–42. 1988a.

Steinmüller, Wilhelm (Hg.): *Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft*. Fischer Taschenbuch Verlag, Frankfurt am Main, 1988b.

Steinmüller, Wilhelm: *Riskante Netze: Informations- und Kommunikationstechnik zwischen Technologie-Abschätzung und Technik-Gestaltung*. R. Oldenbourg Verlag, Wien, München, 1990.

Steinmüller, Wilhelm: *Informationstechnologie und Gesellschaft: Einführung in die angewandte Informatik*. Wissenschaftliche Buchgesellschaft, Darmstadt, 1993.

Steinmüller, Wilhelm: Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann. In: *Recht der Datenverarbeitung*, S. 158–161, 2007.

Steinmüller, Wilhelm, Ermer, Leonhard und Schimmel, Wolfgang: *Datenschutz bei riskanten Systemen*, Band 13 von *Informatik-Fachberichte*. Springer, Berlin, Heidelberg, New York, 1978.

Steinmüller, Wilhelm, Lutterbeck, Bernd, Mallmann, Christoph, Harbort, Uwe, Kolb, Gerhard und Schneider, Jochen: Grundfragen des Datenschutzes. Gutachten, Bundesministerium des Innern, 1971. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1.

Steinmüller, Wilhelm und Wolter, Henner: Besonderheiten elektronischer Datenverarbeitung. In: Dammann, Ulrich, Karhausen, Mark O., Müller, Paul J. und Steinmüller, Wilhelm (Hg.) *Datenbanken und Datenschutz*, Herder & Herder, Frankfurt am Main, S. 51–61. 1974.

Stewart, Blair: Privacy impact assessments. In: *Privacy Law and Policy Reporter*, 1996. URL `http://www.austlii.edu.au/au/journals/PLPR/1996/39.html`.

Stigler, George J.: An Introduction to Privacy in Economics and Politics. In: *The Journal of Legal Studies*, Band 9(4): S. 623–644, 1980.

Stone, M. G. und Warner, Malcolm: Politics, Privacy, and Computers. In: *The Political Quarterly*, Band 40(3): S. 256–267, 1969.

Strathoff, Pepe und Lutz, Christoph: Gemeinschaft schlägt Gesellschaft – Die vermeintliche Paradoxie des Privaten. In: Hahn, Oliver, Hohlfeld, Ralf und Knieper, Thomas (Hg.) *Digitale Öffentlichkeit(en)*. UVK Verlagsgesellschaft, Konstanz, 2015, Band 42 von *Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft*, S. 203–216.

Strömholm, Stig: *Right of Privacy and Rights of the Personality*, Band VIII von *Acta Instituti Upsaliensis Iurisprudentiae Comparativae*. P. A. Norstedt & Söners Förlag, Stockholm, 1967. Working Paper prepared for the Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm May 1967.

Such, Manfred und Fraktion Bündnis 90/Die Grünen: *Entwurf eines Bundesdatenschutzgesetzes (BDSG)*. Deutscher Bundestag, Drs. 13/9082, 1997.

Sundar, S. Shyam und Marathe, Sampada S.: Personalization versus Customization: The Importance of Agency, Privacy, and Power Usage. In: *Human Communication Research*, Band 36: S. 298–322, 2010.

Sweeney, Latanya: Achieving k-Anonymity Privacy Protection Using Generalization and Suppression. In: *International Journal of Uncertainty Fuzziness and Knowledge-Based Systems*, Band 10(5): S. 571–588, 2002a.

Sweeney, Latanya: k-Anonymity: A Model for Protecting Privacy. In: *International Journal of Uncertainty Fuzziness and Knowledge-Based Systems*, Band 10(5): S. 557–570, 2002b.

Swire, Peter: U.S. Senate Committee on Commerce, Science & Transportation. In: *Hearing: „The Need for Privacy Protections: Is Industry Self-Regulation Adequate?“*. 2012.

Swire, Peter: US Surveillance Law, Safe Harbor, and Reforms Since 2013. Research Paper No. 36, Georgia Institute of Technology, Scheller College of Business, Atlanta, 2015.

Tække, Jesper: Digital panopticism and organizational power. In: *Surveillance & Society*, Band 8(4): S. 441–454, 2011.

Task Force on Privacy and Computers: *Privacy and Computers.* Information Canada, Ottawa, 1972.

Tauss, Jörg, Kollbeck, Johannes und Fazlic, Nermin: Modernisierung des Datenschutzes: Wege aus der Sackgasse. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 41–70. 2004.

Tavani, Herman T.: Information Privacy: Concepts, Theories, and Controversies. In: Himma, Kenneth Einar und Tavani, Herman T. (Hg.) *The Handbook of Information and Computer Ethics*, John Wiley & Sons, New York, S. 131–164. 2008.

Tene, Omer und Polonetsky, Jules: Privacy in the Age of Big Data: A Time for Big Decisions. In: *Stanford Law Review*, Band 64: S. 63–69, 2012.

Tene, Omer und Polonetsky, Jules: Judged by the Tin Man: Individual Rights in the Age of Big Data. In: *Journal of Telecommunications and High Technology Law*, Band 11: S. 351–477, 2013.

Tiedemann, Klaus und Sasse, Christoph: *Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft.* Carl Heymanns Verlag KG, Köln, Berlin, Bonn, München, 1973.

Tinnefeld, Marie-Theres, Buchner, Benedikt und Petri, Thomas B.: *Einführung in das Datenschutzrecht.* Oldenbourg Verlag, München, fünfte Auflage, 2012.

Tinnefeld, Marie-Theres, Ehmann, Eugen und Gerling, Rainer W.: *Einführung in das Datenschutzrecht.* Oldenbourg Verlag, München, vierte Auflage, 2005.

Titus, James P.: Security and privacy. In: *Communications of the ACM*, Band 10: S. 379–381, 1967.

Troncoso, Carmela: *Design and analysis methods for privacy technologies.* Dissertation, Department of Electrical Engineering (ESAT), Faculty of Engineering, Katholieke Universiteit Leuven, Leuven, 2011.

Tuner, Lotte: Die Bedeutung des Formularwesens für den Datenschutz. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 254–267. 1976.

Turn, Rein und Ware, Willis H.: Privacy and Security in Computer Systems. Paper P-5361, The RAND Corporation, Santa Monica, California, 1975.

Turow, Joseph, Hoofnagle, Chris Jay, Mulligan, Deirdre K, Good, Nathaniel und Grossklags, Jens: The FTC and Consumer Privacy in the Coming Decade. In: *I/S: A Journal of Law and Policy for the Information Society*, Band 3(3): S. 723–749, 2006.

Tönnies, Ferdinand: *Gemeinschaft und Gesellschaft.* Fues's Verlag, Leipzig, 1887.

ULD, GP: Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen. Abschlussbericht Az.: 314-06.01-2812HS021, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), GP Forschungsgruppe, 2014.

Ulrich, Otto: Leitbildwechsel: dem (sicherheits-)technologisch geprägten Datenschutz gehört die Zukunft. In: *Datenschutz und Datensicherheit*, Band 20(11): S. 664–671, 1996.

U.S. Department of Health, Education, and Welfare: *Records, Computers, and the Rights of Citizens.* The Massachusetts Institute of Technology, 1973.

van Blarkom, G. W., Borking, John J. und Olk, J. G. E.: *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents.* PISA Consortium, Den Haag, 2003.

van den Haag, Ernest: On Privacy. In: Pennock, J. Roland und Chapman, John W. (Hg.) *Privacy*, Atherton Press, New York, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy*, S. 149–168. 1971.

van Goethem, Tom, Piessens, Frank, Joosen, Wouter und Nikiforakis, Nick: Clubbing Seals: Exploring the Ecosystem of Third-party Security Seals. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014, S. 918–929.

van Lamsweerde, Axel: Goal-Oriented Requirements Engineering: A Guided Tour. In: *Proceedings Fifth IEEE International Symposium on Requirements Engineering, 2001*. IEEE, 2001, S. 249–262.

van Lamsweerde, Axel: Requirements Engineering: From Craft to Discipline. In: *Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of software engineering*. ACM, 2008, S. 238–249.

van Rest, Jeroen, Boonstra, Daniel, Everts, Maarten, van Rijn, Martin und van Paassen, Ron: Designing Privacy-by-Design. In: Preneel, Bart und Ikonomou, Demosthenes (Hg.) *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers*. Springer, Berlin, 2014, S. 55–72.

van Rossum, Henk, Gardeniers, Huib, Borking, John, Cavoukian, Ann, Brans, John, Muttupulle, Noel und Magistrale, Nick: *Privacy-Enhancing Technologies: The Path to Anonymity*. Information and Privacy Commissioner / Ontario, Canada & Registratiekamer, The Netherlands, Den Haag, 1995.

Vec, Miloš: Kurze Geschichte des Technikrechts. In: Schulte, Martin, Schröder, Rainer, Honsell, H. und Lerche, P. (Hg.) *Handbuch des Technikrechts*, Springer, Berlin, Heidelberg, S. 3–92. Zweite Auflage, 2011.

Vedder, Anton: KDD: The challenge to individualism. In: *Ethics and Information Technology*, Band 1(4): S. 275–281, 1999.

Vesting, Thomas: Das Internet und die Notwendigkeit der Transformation des Datenschutzes. In: Ladeur, Karl-Heinz (Hg.) *Innovationsoffene Regulierung des Internet*, Nomos Verlagsgesellschaft, Baden-Baden, S. 155–190. 2003.

Victor, Jacob M.: The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. In: *Yale Law Journal*, Band 123(2): S. 266–529, 2013.

Vila, Tony, Greenstadt, Rachel und Molnar, David: Why We Can't Be Bothered to Read Privacy Policies – Models of Privacy Economics as a Lemons Market. In: *Proceedings of the 5th international conference on Electronic commerce*. ACM, 2003, S. 403–407.

von Alemann, Ulrich und Schatz, Heribert: *Mensch und Technik: Grundlagen und Perspektiven einer sozialverträglichen Technikgestaltung*, Band 1 von *Sozialverträgliche Technikgestaltung*. Westdeutscher Verlag, Opladen, zweite Auflage, 1987.

von Berg, Malte: *Automationsgerechte Rechts- und Verwaltungsvorschriften*. G. Grote'sche Verlagsbuchhandlung KG, Köln, Berlin, 1968.

von Berg, Malte: Datenverbund in der öffentlichen Verwaltung. In: Schmitz, P. (Hg.) *Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung*. Gesellschaft für Informatik, Fachausschuß 8 „Methoden der Informatik für spezielle Anwendungen", Springer, Berlin, Heidelberg, New York, 1974, Band 9 von *Lecture Notes in Computer Science*, S. 70–74.

von Berg, Malte, Harboth, Uwe, Jarass, Hans D. und Lutterbeck, Bernd: Schafft die Datenverarbeitung den modernen Leviathan? In: *Öffentliche Verwaltung und Datenverarbeitung*, Band 2(1): S. 3–7, 1972.

von Gierke, Otto: *Deutsches Privatrecht*, Band 1. Verlag von Duncker & Humblot, Leipzig, 1895. Karl Bindig: Systematisches Handbuch der Deutschen Rechtswissenschaft. Zweite Abteilung, dritter Teil, erster Band.

von Grafenstein, Maximilian: Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit. Zur mangelnden Differenzierung der Rechtsgüterbetroffenheit in der Datenschutzgrund-VO. In: *Datenschutz und Datensicherheit*, Band 39(12): S. 789–795, 2015.

von Lewinski, Kai: Geschichte des Datenschutzrechts von 1600 bis 1977. In: Arndt, Felix (Hg.) *Freiheit – Sicherheit – Öffentlichkeit*. Nomos Verlagsgesellschaft, 2009, 48. Assistententagung Öffentliches Recht, S. 196–220.

von Lewinski, Kai: Kodifikationsstrategien im Datenschutzrecht, oder: Wann ist der Zeitpunkt der Unkodifizierbarkeit erreicht? In: Kloepfer, Michael (Hg.) *Gesetzgebung als wissenschaftliche Herausforderung. Gedächtnisschrift für Thilo Brandner*, Nomos Verlagsgesellschaft, Baden-Baden, S. 107–121. 2011.

von Lewinski, Kai: Europäisierung des Datenschutzrechts. In: *Datenschutz und Datensicherheit*, Band 36(8): S. 564–570, 2012.

von Lewinski, Kai: *Die Matrix des Datenschutzes. Besichtigung und Ordnung eines Begriffsfeldes*, Band 1 von *Internet und Gesellschaft*. Mohr Siebeck, Tübingen, 2014.

von Lewinski, Kai: Zufall und Notwendigkeit bei der Entstehung des Datenschutzrechts. Was sagt die kontrafaktische Geschichtsschreibung zum BDSG? In: Pohle, Jörg und Knaut, Andrea (Hg.) *Fundationes I: Geschichte und Theorie des Datenschutzes*. Monsenstein und Vannerdat, Münster, 2014, S. 9–35.

von Mutius, Albert: Verfassungsrechtliche Grenzen der Einwilligung im Datenschutzrechts. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 101–128. 2004.

von Stechow, Constantin: *Datenschutz durch Technik – Rechtliche Förderungsmöglichkeiten von Privacy Enhancing Technologies am Beispiel der Videoüberwachung*. Deutscher Universitäts-Verlag, 2005.

Wagner, Edgar: Verfalldatum für Internet-Speicherungen? In: *Datenschutz und Datensicherheit*, Band 32(1): S. 6–6, 2008.

Wagner, Isabel und Eckhoff, David: Technical Privacy Metrics: A Systematic Survey. In: *arXiv preprint arXiv:1512.00327*, 2015.

Waidner, Michael: *Datenschutz und Betrugssicherheit garantierende Kommunikationsnetze: Systematisierung des Datenschutzmassnahmen und Ansätze zur Verifikation der Betrugssicherheit*. Diplomarbeit, Universität Karlsruhe, Fakultät für Informatik, Institut für Informatik IV, Kralsruhe, 1985. Auch: Interner Bericht 19/85.

Waidner, Michael und Pfitzmann, Andreas: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen. In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 128–141. 1985.

Waidner, Michael und Pfitzmann, Birgit: Anonyme und verlusttolerante elektronische Brieftaschen. Interner Bericht 1, Universität Karlsruhe, Fakultät für Informatik, Institut für Rechnerentwurf und Fehlertoleranz, Karlsruhe, 1987.

Ware, Willis H.: Security and privacy in computer systems. In: *Proceedings of the April 18-20, 1967, spring joint computer conference*. ACM, New York, NY, USA, 1967a, AFIPS '67 (Spring), S. 279–282.

Ware, Willis H.: Security and privacy: similarities and differences. In: *Proceedings of the April 18-20, 1967, spring joint computer conference*. ACM, New York, NY, USA, 1967b, AFIPS '67 (Spring), S. 287–290.

Warner, Malcolm und Stone, Michael: *The Data Bank Society: Organizations, Computers and Social Freedom*. George Allen & Unwin Ltd., London, 1970.

Warren, Adam, Bayley, Robin, Bennett, Colin J., Charlesworth, Andrew, Clarke, Roger A. und Oppenheim, Charles: Privacy Impact Assessment: International experience as a basis for UK Guidance. In: *Computer Law & Security Report*, Band 24: S. 233–242, 2008.

Warren, Samuel D. und Brandeis, Louis D.: The Right to Privacy. In: *Harvard Law Review*, S. 193–220, 1890.

Watzlawick, Paul, Beavin, Janet Helmick und Jackson, Don D.: *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes*. W. W. Norton & Company, Inc., New York, 1967.

Weber, Hermann: 48. Deutscher Juristentag in Mainz. In: *Juristische Schulung*, Band 10(12): S. 644–649, 1970.

Weber, Max: *Schriften zur Soziologie*. Philipp Reclam jun., Stuttgart, 1995.

Weber, Rolf H.: Internet of things: Privacy issues revisited. In: *Computer Law & Security Review*, Band 31(5): S. 618–627, 2015.

Wegscheider, Herbert: Die Begriffsbestimmungen der Regierungsvorlage zum österreichischen Datenschutzgesetz. In: Dierstein, Rüdiger, Fiedler, Herbert und Schulz, Arno (Hg.) *Datenschutz und Datensicherung*, J. P. Bachem Verlag, Köln, S. 83–97. 1976.

Weichert, Thilo: Datenschutzberatung – Hilfe zur Selbsthilfe. In: Bäumler, Helmut (Hg.) *„Der neue Datenschutz" – Datenschutz in der Informationsgesellschaft von morgen*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 213–229. 1998.

Weichert, Thilo: Der Entwurf eines Bundesdatenschutzgesetzes von BÜNDNIS90/DIE GRÜNEN. In: Bäumler, Helmut und von Mutius, Albert (Hg.) *„Datenschutzgesetze der dritten Generation": Texte und Materialien zur Modernisierung des Datenschutzrechts*, Hermann Luchterhand Verlag, Neuwied, Kriftel, S. 78–91. 1999.

Weichert, Thilo: Zur Ökonomisierung des Rechts auf informationelle Selbstbestimmung. In: Bäumler, Helmut (Hg.) *E-Privacy: Datenschutz im Internet*, Vieweg, Braunschweig/Wiesbaden, S. 158–184. 2000.

Weichert, Thilo: Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung. In: *Neue Juristische Wochenschrift*, (20): S. 1463–1469, 2001.

Weichert, Thilo: Datenschutz, der Spaß macht. In: Bizer, Johann, von Mutius, Albert, Petri, Thomas B. und Weichert, Thilo (Hg.) *Innovativer Datenschutz 1992 – 2004. Wünsche, Wege, Wirklichkeit. Für Helmut Bäumler*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, S. 129–146. 2004.

Weichert, Thilo: Der Personenbezug von Geodaten. In: *Datenschutz und Datensicherheit*, Band 31(2): S. 113–119, 2007.

Weichert, Thilo: Wider das Verbot mit Erlaubnisvorbehalt im Datenschutz? In: *Datenschutz und Datensicherheit*, Band 37(4): S. 246–249, 2013.

Weinstein, Michael A.: The Uses of Privacy in the Good Life. In: Pennock, J. Roland und Chapman, John W. (Hg.) *Privacy*, Atherton Press, New York, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy*, S. 88–104. 1971a.

Weinstein, W. L.: The Private and the Free: A Conceptual Inquiry. In: Pennock, J. Roland und Chapman, John W. (Hg.) *Privacy*, Atherton Press, New York, Band XIII von *NOMOS. Yearbook of the American Society for Political and Legal Philosophy*, S. 27–55. 1971b.

Weise, Karl Theodor: Was ist übertriebener Datenschutz? In: Gola, Peter (Hg.) *Datenschutz im Konflikt*, J. Schweitzer Verlag, München, Beiheft 13, Datenverarbeitung im Recht (DVR), S. 129–136. 1983.

Weizenbaum, Joseph: *Computer Power and Human Reason.* W. H. Freeman and Company, San Francisco, 1976.

Wesel, Uwe: hM. In: *Kursbuch*, Band 56: S. 88–109, 1979.

Westin, Alan F.: Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I—The Current Impact of Surveillance on Privacy. In: *Columbia Law Review*, Band 66(6): S. 1003–1050, 1966a.

Westin, Alan F.: Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part II—Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance. In: *Columbia Law Review*, Band 66(7): S. 1205–1253, 1966b.

Westin, Alan F.: *Privacy and Freedom.* Atheneum, New York, 1967.

Westin, Alan F. und Baker, Michael A.: *Databanks in a Free Society: Computers, Record-Keeping and Privacy.* Quadrangle / The New York Times Book Co., 1972.

White, Gregory L. und Zimbardo, Philip G.: The Chilling Effects of Surveillance: Deindividuation and Reactance. ONR Technical Report Z-15, Office of Naval Research, Los Angeles, 1975.

Whitman, James Q.: The Two Western Cultures of Privacy: Dignity versus Liberty. In: *The Yale Law Journal*, Band 113(6): S. 1151–1221, 2004.

Whyte, William H., jr.: *The Organization Man.* Simon and Schuster, New York, 1956.

Willis, Lauren E.: Why Not Privacy by Default. In: *Berkeley Technology Law Journal*, Band 29: S. 61–133, 2014.

Windolph, Albert: Zur Problematik des Entwurfs eines Bundesdatenschutzgesetzes. In: Schmitz, P. (Hg.) *Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung.* Gesellschaft für Informatik, Fachausschuß 8 „Methoden der Informatik für spezielle Anwendungen“, Springer, Berlin, Heidelberg, New York, 1974, Band 9 von *Lecture Notes in Computer Science*, S. 215–224.

Winner, Langdon: Do Artifacts Have Politics? In: *Daedalus*, Band 109(1): S. 121–136, 1980.

Winograd, Terry und Flores, Fernando: *Understanding Computers and Cognition.* Ablex, Chicago, 1986.

Woertge, Hans-Georg: *Die Prinzipien des Datenschutzrechts und ihre Realisierung im geltenden Recht.* R. v. Decker's Verlag, G. Schenk, Heidelberg, 1984.

Wright, David und De Hert, Paul (Hg.): *Privacy Impact Assessment.* Springer, Berlin, 2012.

Wright, David und Raab, Charles D.: Constructing a surveillance impact assessment. In: *Computer Law & Security Review*, Band 28(6): S. 613–626, 2012.

Wright, Steve: An appraisal of technologies for political control. Working document PE 166 499, STOA – Scientific and Technological Options Assessment, European Parliament, Luxemburg, 1998.

Wächter, Michael: Datenschutz als „Software-Routine“. In: *Datenschutz und Datensicherheit*, Band 20(5): S. 272–278, 1996.

Young, Alyson Leigh und Quan-Haase, Anabel: Privacy Protection Strategies on Facebook: The Internet privacy paradox revisited. In: *Information, Communication & Society*, Band 16(4): S. 479–500, 2013.

Younger, Kenneth: Report of the Committee on Privacy. Report Cmnd 5012, HMSO, London, 1972.

Yu, Eric und Cysneiros, Luiz Marcio: Designing for Privacy and Other Competing Requirements. In: *Proceedings of the 3rd Symposium on Requirements Engineering for Information Security*. 2002, S. 5:1–5:15.

Yu, Eric und Cysneiros, Luiz Marcio: Designing for Privacy in a Multi-agent World. In: Falcone, Rino, Barber, Suzanne, Korba, Larry und Singh, Munindar (Hg.) *Trust, Reputation, and Security: Theories and Practice.* Berlin, 2003, Band 2631 von *Lecture Notes in Computer Science*, S. 209–223.

Zalnieriute, Monika: An international constitutional moment for data privacy in the times of mass-surveillance. In: *International Journal of Law and Information Technology*, Band 23(2): S. 99–133, 2015.

Zanfir, Gabriela: Forgetting About Consent. Why The Focus Should Be On „Suitable Safeguards“ in Data Protection Law. In: Gutwirth, Serge, Leenes, Ronald und De Hert, Paul (Hg.) *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*. Springer, Dordrecht, 2014, S. 237–257.

Zanfir, Gabriela: Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The „New Clothes“ of an Old Right. In: Gutwirth, Serge, Leenes, Ronald und De Hert, Paul (Hg.) *Reforming European Data Protection Law*. Springer, Dordrecht, 2015.

Zarsky, Tal: Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond. In: Gutwirth, Serge, Poullet, Yves und De Hert, Paul (Hg.) *Data Protection in a Profiled World*. Springer, Dordrecht, 2010, S. 53–74.

Zarsky, Tal: Understanding Discrimination in the Scored Society. In: *Washington Law Review*, Band 89(4): S. 1375–1412, 2014.

Ziegeldorf, Jan Henrik, Morchon, Oscar García und Wehrle, Klaus: Privacy in the Internet of Things: threats and challenges. In: *Security and Communication Networks*, Band 7(12): S. 2728–2742, 2014.

Ziegler-Jung, Bärbel: Verfahrensregelungen und Selbstregulierung der speichernden Stelle – Rechtliche Lösungsmöglichkeiten von Datenschutzproblemen? In: Spies, Peter Paul (Hg.) *Datenschutz und Datensicherung im Wandel der Informationstechnologien*, Springer-Verlag, Berlin, Band 113 von *Informatik-Fachberichte*, S. 250–256. 1985.

Zilkens, Martin: *Datenschutz in der Kommunalverwaltung*. Erich Schmidt Verlag, Berlin, zweite Auflage, 2008.

Zimmermann, Wolfgang: Privatsphäre. Aufruf zur Konstruktion einer realitätsbezogenen Bildwelt. In: Pohle, Jörg und Knaut, Andrea (Hg.) *Fundationes I: Geschichte und Theorie des Datenschutzes*. Monsenstein und Vannerdat, Münster, 2014, S. 45–63.

Zuboff, Shoshana: *In the Age of the Smart Machine: The Future of Work and Power*. Basic Books, New York, NY, 1988.

Zuboff, Shoshana: Big other: surveillance capitalism and the prospects of an information civilization. In: *Journal of Information Technology*, Band 30(1): S. 75–89, 2015.